



Marcia E. Asquith
Executive Vice President,
Board and External Relations

[REDACTED]
Fax: (202) 728-8300

November 30, 2020

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

Via Email to rule-comments@sec.gov

Re: Comment Letter on Securities Exchange Act Release No. 89632 – Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail (“CAT”) to Enhance Data Security (File No. S7-10-20)

Dear Ms. Countryman:

The Financial Industry Regulatory Authority, Inc. (“FINRA”)¹ appreciates this opportunity to comment on the Securities and Exchange Commission’s (“Commission” or “SEC”) proposed amendments to the CAT NMS Plan to enhance data security (the “Proposal”).² FINRA fully supports the main objective of the Proposal—namely, enhanced security and confidentiality of data submitted to CAT (“CAT Data”).³ As CAT

¹ FINRA is submitting this letter solely in its capacity as a Participant of the National Market System Plan Governing the Consolidated Audit Trail (the “CAT NMS Plan” or “Plan”). This letter does not reflect or represent the views of FINRA CAT, LLC, which is a distinct corporate subsidiary of FINRA that acts as the CAT Plan Processor pursuant to an agreement with the Plan Participants. To the extent feedback on the Proposal is provided from FINRA CAT, LLC’s perspective, FINRA understands it may be reflected in separate comment letters submitted by FINRA CAT, LLC or jointly by the Participants.

² See Securities Exchange Act Release No. 89632 (August 21, 2020), 85 FR 65990 (October 16, 2020).

³ As discussed further below, the term “CAT Data” is defined broadly in Section 1.1 of the CAT NMS Plan to mean “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.”

implementation builds on recent progress and CAT reporting continues to be phased in successfully, FINRA welcomes the Proposal as an important step in the collective efforts of the CAT NMS Plan Participants, the Commission, and market participants to continually evaluate CAT Data security while preserving the utility of CAT as a regulatory tool.

FINRA believes achieving the right balance of CAT security and regulatory utility is critical. The CAT System⁴ and CAT Data must remain as secure as possible, yet regulators must be allowed sufficient and effective access to CAT Data if the CAT is to serve its core purpose of enhancing market supervision. FINRA believes this balance is recognized by the Proposal's approach to programmatic access to customer and account information, which FINRA generally supports (although it requests clarification in certain areas). Similarly, FINRA supports the Proposal's requirement to locate analysis of CAT Data within secure analytical workspaces ("SAWs") that are subject to centralized monitoring as well as common, independently audited controls. Importantly, however, FINRA believes the Proposal's key security objectives can be met without centralizing ownership and provision of SAW accounts within the CAT System. In fact, FINRA believes that such centralized SAW ownership could create additional risks that may undermine both the security of CAT and its regulatory purpose. The important data security objectives of the Proposal should not (and need not) be achieved in a manner that increases certain risks to the CAT System or diminishes the extensive market oversight that FINRA is able to perform today, as described more fully below.

FINRA's support for the objectives of the Proposal is detailed below, along with discussion of a modified SAW framework alternative that FINRA believes would more optimally balance CAT Data security and FINRA's regulatory use. In addition, this letter identifies several aspects of the Proposal that FINRA believes remain uncertain and would benefit from further clarification. FINRA notes, however, that given the complexity of the Proposal and the variable downstream impacts it may have on FINRA's overall security measures and core regulatory workflows, it is difficult to address all of its interrelated components in a static written letter. Accordingly, FINRA believes further dialogue with SEC staff is needed if the Proposal moves forward. Such FINRA/SEC staff dialogue would better facilitate in-depth discussion of the methods that FINRA uses to integrate audit trail data into its regulatory systems and programs, and the ways that certain elements of the Proposal could reduce the effectiveness of FINRA's regulatory programs.

⁴ The term "CAT System" is defined in Section 1.1 of the CAT NMS Plan to mean "all data processing equipment, communications facilities, and other facilities, including equipment, utilized . . . in connection with [the] operation of the CAT and any related information or relevant systems pursuant to [the CAT LLC Agreement]."

I. Background

A. *FINRA's Role in Market Supervision*

FINRA, a not-for-profit self-regulatory organization (“SRO”), is registered with the Commission as a national securities association under Section 15A of the Securities Exchange Act of 1934 (the “Exchange Act” or “Act”).⁵ FINRA does not operate a market or otherwise execute transactions that are reported to CAT. Under the Exchange Act, FINRA has statutory responsibility for the regulation and supervision of member broker-dealers, including broker-dealers’ off-exchange activities. In particular, FINRA is required under Section 19(g)(1) of the Exchange Act to enforce compliance by its members and persons associated with its members with the Exchange Act, the rules and regulations thereunder, and FINRA’s own rules. As an SRO, FINRA must have rules “designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.”⁶

The SEC has stated that an SRO’s responsibility to enforce compliance under Section 19(g)(1) “necessarily includes an obligation to monitor and maintain surveillance over its members.”⁷ The SEC has explained further that “[w]hen these surveillance efforts identify suspicious trading activity, SROs have a responsibility to open investigations in which they assemble and review additional market data to assess the nature and scope of the potential misconduct.”⁸

To meet FINRA’s obligations to supervise the securities activities of its members wherever they take place, and to advance its mission of investor protection and market integrity, FINRA performs the full range of market supervision functions: surveillance, examinations, investigations, and enforcement. FINRA does this work both on its own behalf and on behalf of national securities exchanges pursuant to regulatory services

⁵ 15 U.S.C. 78o-3.

⁶ 15 U.S.C. 78o-3(b)(6).

⁷ *See, e.g.*, In the Matter of Chicago Stock Exchange, Exchange Act Release No. 48566 (Sept. 30, 2003).

⁸ *See* Securities Exchange Act Release No. 67457 (July 18, 2012), 77 FR 45722, 45727 (August 1, 2012) (“Rule 613 Adopting Release”).

agreements (“RSAs”) and agreements under Rule 17d-2 of the Exchange Act.⁹ Under these arrangements, FINRA developed an extensive and sophisticated cross-market supervision program that, before CAT, already covered 100% of U.S. equity market activity and approximately 45% of options contract volume. In addition to the cross-market supervision services FINRA provides under these agreements, FINRA provides market-specific regulatory services to several exchanges.

FINRA uses this range of supervisory tools to enforce compliance with a variety of rules. In the cross-market space, this includes regulatory supervision of rules that prohibit manipulation (including layering and spoofing) and rules that address different types of cross-market conduct (including best execution, limit order display, trading ahead of customer orders, SEC Regulation M, SEC Regulation NMS Rules 610 and 611, SEC Regulation SHO, SEC Rule 15c3-5, and the CAT reporting compliance rules). In addition, FINRA conducts surveillance and investigations on behalf of the U.S. exchanges in enforcing rules prohibiting insider trading, manipulation and fraud, and in certain cases as noted above, market-specific rules (including exchange-specific rules on the opening and closing process and market maker quoting obligations).

B. CAT Implementation and Enhanced Market Supervision Efforts

A central purpose of the CAT is to enhance the data available to regulators for their use in market supervision. When the Commission approved the CAT NMS Plan, it noted that “[t]he purpose of the Plan, and the creation, implementation and maintenance of a comprehensive audit trail for the U.S. securities markets described therein, is to ‘substantially enhance the ability of the SROs and the Commission to oversee today’s securities markets and fulfill their responsibilities under the federal securities laws.’”¹⁰ In particular, the CAT is meant to improve regulators’ ability to perform market reconstruction and analysis and to conduct market surveillance, examinations, investigations, and enforcement functions.¹¹ To support this goal, the Participants are required to implement new or enhanced surveillance systems to make use of CAT Data.¹²

⁹ When FINRA provides regulatory services to an exchange under an RSA, the exchange retains ultimate regulatory responsibility and reviews FINRA’s performance of the services provided under the RSA.

¹⁰ See Securities Exchange Act Release No. 79318 (November 15, 2016), 81 FR 84696, 84698 (November 23, 2016) (“CAT NMS Plan Approval Order”).

¹¹ See *id.* at 84833.

¹² See CAT NMS Plan, Sections 6.7 and 6.10; see also Rule 613 (a)(3)(iv) of SEC Regulation NMS.

As the Commission noted recently, CAT implementation is well underway, with concrete progress and the achievement of key initial industry reporting milestones.¹³ Accordingly, with CAT implementation progressing through its phased implementation of order and transaction data reporting, FINRA has dedicated substantial resources in an ongoing effort to integrate CAT Data into its regulatory systems. Given the breadth of FINRA's regulatory activities and services, CAT Data integration is a complex undertaking that requires extensive changes both to FINRA's technology systems and regulatory workflows. FINRA has already developed a substantial portion of a new consolidated data platform on which its surveillance patterns will run—notably, this data platform must include not only CAT Data, but also the additional data that FINRA uses to enrich the audit trail so that it can perform surveillance more effectively. FINRA is also undertaking a significant effort to migrate its surveillance program to the new data platform. Upon the full implementation of customer and account information reporting scheduled for 2022, FINRA expects it will make substantial additional investments to continue its surveillance enhancements and CAT Data integration.

In addition to these efforts to integrate CAT Data into FINRA's regulatory tools to detect potential misconduct, FINRA developed a new CAT Industry Member reporting compliance program to ensure the CAT's data integrity. This new CAT reporting compliance program—which FINRA operates on behalf of all the Participants¹⁴—involves its own new suite of surveillance patterns deployed on FINRA's new data platform, as well as increased staffing to conduct corresponding examinations, investigations, and enforcement.

C. FINRA's Commitment to CAT Data Security

FINRA is fully committed to integrating CAT Data into its regulatory programs in a secure manner. Protecting sensitive data is not new for FINRA. Since FINRA began operating OATS—the predecessor to CAT—FINRA has expanded its use of various data sources to develop sophisticated surveillance capabilities relied on by the Commission, other federal and state regulators and SROs, and market participants more broadly. Critically, security has been an integral component of FINRA's regulatory efforts throughout, and FINRA has a proven track record using sensitive data effectively and securely.

¹³ See Jay Clayton, Brett Redfearn, & Manisha Kimmel, Public Statement, Update on the Consolidated Audit Trail: Data Security and Implementation Progress (August 21, 2020), available at <https://www.sec.gov/news/public-statement/clayton-kimmel-redfearn-nms-cat-2020-08-21>.

¹⁴ See *Regulatory Notice* 20-20 (June 2020) (discussing the Participants' efforts to coordinate regulation of the CAT reporting compliance rules through FINRA).

FINRA has leveraged its experience and expertise to ensure the secure integration of CAT Data within its controlled environment. FINRA uses both architectural-level and program-level security controls in its own environment that align with industry standards, including National Institute of Standards and Technology (“NIST”) Special Publication (“SP) 800-53. FINRA’s existing security controls address the same range of issues required by the Plan for the CAT System, including data storage and handling, insider risk, data connectivity and transfer, incident management, security logging and monitoring, and account management. Furthermore, FINRA’s security controls are subject to multiple layers of external review—they have been reviewed by the FINRA CAT Chief Information Security Officer (“CISO”) as required by the Plan and deemed comparable to the controls in place for the CAT System; they are reviewed in the course of FINRA’s regular external Service Organizational Control (“SOC”) audits; and they are designed to meet the requirements of Regulation Systems Compliance and Integrity (“Regulation SCI”) and subject to regular examinations for compliance by the SEC’s Technology Controls Program.

Building on these controls, as the Commission discusses in the Proposal, FINRA is also already working to implement a SAW within FINRA’s cloud-hosted environment for the controlled and monitored analysis of CAT Data. Before the SEC published the Proposal, the Participants and FINRA CAT developed a SAW concept with published requirements approved by the CAT Operating Committee. These current SAW requirements were developed by the Plan Participants and FINRA CAT, in consultation with the CAT’s Security Working Group (“SWG”), prior to Operating Committee approval. At a high level, the current SAW requirements contemplate the creation of new SAW environments that are owned and managed by each Participant; subject to security controls recommended by FINRA CAT based on FINRA CAT’s system security plan designed for the CAT System; and actively monitored by the Plan Processor for certain perimeter controls and other selected security characteristics. While the current SAW requirements are not mandatory for Participants that take CAT Data into their own environments, FINRA voluntarily committed to comply with the current SAW requirements, and FINRA’s work to implement the current SAW requirements is underway.

Consistent with FINRA’s proven security program and its voluntary commitment to the current SAW requirements, FINRA welcomes the Proposal as an important step to further evaluate potential enhancements to the secure and effective use of CAT as a regulatory tool. While FINRA fully supports the enhanced security objectives of the Proposal, FINRA believes the Commission should modify the Proposal in several ways, as discussed below.

II. Support for a Modified SAW Framework That Relies on Central Monitoring Rather Than Central Ownership

A. Challenges with the Proposal’s Centralized SAW Ownership Framework

As noted above, FINRA is already working to implement a SAW for CAT Data. The Commission recognized these efforts in the Proposal, although it noted several concerns it had with the current SAW framework. Specifically, the Commission noted that:

Use of such environments is currently optional; the Participants are not required to use the analytic environments built by the Plan Processor when accessing and analyzing Customer and Account Attributes and, without the proposed amendments, could continue to access large amounts of CAT Data outside of these controlled environments. The Commission also understands that the security controls for these analytic environments would not be implemented by one centralized party. Rather, each Participant would be responsible for the selection and implementation of security controls for its own analytic environments.¹⁵

To address these concerns, the Proposal establishes an entirely new SAW framework built around centralized SAW ownership and provisioning by the Plan Processor within the CAT System. The centralized ownership and provisioning of SAW accounts by the Plan Processor is intended to minimize the CAT's attack surface, maximize security-driven monitoring of CAT Data, and to leverage, wherever possible, security controls and related policies and procedures that are consistent with those that protect the CAT Central Repository.¹⁶

FINRA supports the Commission's objectives and agrees that SAW usage for CAT Data analysis should be mandatory. However, FINRA sees a number of challenges with the Proposal's new framework for centralized SAW ownership by the Plan Processor within the CAT System. Most importantly, FINRA believes it is simply not feasible to operate its full regulatory environment within a centrally-owned SAW framework, and doing so would create substantial unintended risks both to CAT security and FINRA's regulatory performance.

As discussed above, FINRA meets its broad regulatory obligations by operating a complex network of interrelated systems that draw on data from a variety of sources. If FINRA were to disconnect and relocate certain systems to a new SAW account centrally owned and provisioned by the Plan Processor, it would cause significant disruption to FINRA's various regulatory workflows, particularly given the additional data that FINRA uses in its environment to enrich CAT data for surveillance, as well as the proposed limitations on extracting data from the SAW. Similarly problematic, if FINRA were to migrate its full suite of systems and data to a centrally-owned SAW within the CAT System—as FINRA believes would be necessary to minimize such disruption to its

¹⁵ Proposal at 66075.

¹⁶ *Id.* at 65995.

workflows—it would undermine a key purpose of the Proposal. Rather than minimizing the attack surface of the CAT, this step would dramatically increase the attack surface by expanding the CAT System perimeter to include the entirety of FINRA’s environment alongside CAT Data. Furthermore, because FINRA necessarily relies on running surveillance that programmatically considers both transaction data and customer-identifying information in databases outside the CAT, particularly for the detection of fraud and insider trading, FINRA would need to bring sensitive customer data into the CAT System, contrary to the efforts of the Participants, industry, and Commission to keep such data out.

A centrally-owned SAW framework poses other risks as well. To relocate FINRA’s regulatory operations into an account within the CAT System, FINRA would need to move significant amounts of proprietary and confidential intellectual property, including sensitive source code, into an account it does not own and manage. Central ownership would also move the location of FINRA’s books and records into an account it does not own and control, which creates additional legal and compliance uncertainty for both FINRA and the Plan Processor.

Moreover, to implement the Proposal’s approach to centralized SAW ownership, the Plan Processor effectively would need to require each Participant to adopt various new standardized policies and procedures—including critical software development lifecycle (“SDLC”) and disaster recovery policies. These policies are essential components of FINRA’s operations and have been developed to serve FINRA’s unique regulatory needs and structure. A move towards such new, standardized policies could both increase operational risk and limit innovation. For example, the need to depart from trusted SDLC policies and adopt new, untested processes could further increase operational risk. FINRA believes this increased risk is unnecessary, particularly given that Participants could still adopt common security controls without the more dramatic SDLC standardization that would be required by centralized SAW ownership. Furthermore, by placing responsibility for a central, standardized SDLC process in the Plan Processor, FINRA is concerned it would be inhibited from deploying new, innovative technology that it relies on to continuously improve its regulatory expertise. FINRA also is concerned that centralized SAW ownership may require the Plan Processor to manage, coordinate, and prioritize far more complex—and potentially conflicting—disaster recovery efforts in the event that multiple Participants needed to fail over to back up environments.

In addition to these regulatory and operational risks, which do not appear accounted for in the Proposal, FINRA also believes the Commission significantly underestimates the costs of migration to a new centrally-owned SAW environment. It is difficult for FINRA to calculate what its costs would be in reality, given the uncertainty noted above about how many systems FINRA would need to move to a centrally-owned SAW. Assuming FINRA would need to migrate at least a substantial portion, if not all, of its environment to avoid regulatory disruption, FINRA projects that its initial implementation costs to comply with the new proposed centrally-owned SAW framework would be at least eight times more

than the \$5.3 million in initial costs that the SEC estimated for FINRA.¹⁷ However, FINRA believes its actual implementation costs reasonably may be far greater than this initial projection, given that the Proposal leaves open a number of other essential questions about the architecture of a centrally-owned SAW framework. For example, the Proposal does not address the likelihood that each Participant would need multiple SAW accounts within the CAT System to segregate development, quality assurance, certification testing, production, and disaster recovery environments. FINRA's actual implementation costs would depend necessarily on resolution of the various material questions that are left open by the Proposal.¹⁸ And notably, the significant monetary investments and related efforts FINRA already has underway to implement the current voluntary SAW requirements could not be leveraged to any significant degree to reduce its costs to adopt the new centrally-owned SAW requirements.¹⁹

Overall, FINRA believes the Proposal materially underestimates the complexity, risks, and costs of a centrally-owned SAW framework. Critically, FINRA's issues with central SAW ownership are not merely a matter of costs, as FINRA has demonstrated its strong commitment to investments in technology and security, illustrated most recently by its efforts to implement the currently voluntary SAW. Rather, FINRA believes it is essential that the Proposal does not diminish FINRA's ability to conduct and enhance its regulatory programs to detect misconduct for potential enforcement or referral to the Commission and other regulators. To better allow for more in-depth discussion of these

¹⁷ See Proposal at 66079 n.664 (estimating FINRA's initial technical development costs at roughly \$1.75 million) and n.674 (estimating FINRA's initial operations implementation costs at roughly \$3.5 million).

¹⁸ For another example, FINRA's initial estimate assumes that it would be permitted to deploy its existing infrastructure tooling and software platforms in a new centrally-owned SAW framework. However, whether FINRA would in fact be permitted to do so would depend under the Proposal on the future development of the Comprehensive Information Security Program ("CISP") and detailed design specifications. If FINRA could not deploy its existing infrastructure tooling and software platforms as assumed, its implementation costs would increase materially.

¹⁹ FINRA notes that the Proposal overstates the degree to which FINRA could leverage its current presence in an Amazon Web Services ("AWS") analytic environment when estimating FINRA's costs to comply with the Proposal. For the reasons discussed in this letter, FINRA believes the proposed move to a new centrally-owned SAW account would require extensive new development, implementation, and migration work, notwithstanding the fact that the new centrally-owned SAW account would also be hosted within AWS. The Commission does not appear to account for this complexity when it applies, without further basis or justification, a 75% discount factor to FINRA's estimated technical development and implementation costs. See Proposal at 66079 n.664 and n.674.

concerns, FINRA welcomes the opportunity to discuss its regulatory use cases with the Commission in further detail.

B. A Modified SAW Framework Alternative Based on Central Monitoring Rather Than Central Ownership

Importantly, FINRA believes centralized SAW ownership by the Plan Processor is not needed to achieve the Proposal's intended benefits. The Proposal identified five benefits of the centrally-owned SAW framework:

First, to the extent that the Plan Processor implements common security controls for SAWs more uniformly than they would be under the current approach, wherein each Participant would be allowed to implement selected security controls for its own analytic environment(s), security may improve by reducing variability in security control implementation, potentially preventing relatively weaker implementations. Second, because implementation of common security controls will be uniform, the proposed amendments may increase the ability of the Plan Processor to conduct centralized and uniform monitoring across all environments from which CAT Data is accessed and analyzed. Third, the Commission preliminarily believes that exceptions to the proposed SAW usage requirements may allow Participants to achieve or maintain the security standards required by the Plan more efficiently. Fourth, the Commission preliminarily believes that provisions in the proposed amendments that provide for a third-party annual review process for the continuance of any exceptions that are granted would provide a procedure and timeline for remedying security deficiencies in [non-SAW excepted environments]. Finally, to the extent that policies and procedures governing data security are less rigorous in application than the security provisions for SAWs in the proposed amendments, data downloaded to SAWs would be more secure than it might be in other analytic environments permitted under the CAT NMS Plan.

FINRA believes that these benefits can be achieved equally by a mandatory SAW framework that retains many of the Proposal's requirements but allows the Participants to retain ownership and control of SAW accounts. Rather than being built on centralized SAW ownership, this modified alternative framework would be built on an SRO controlled SAW environment subject to enhanced central monitoring by the Plan Processor.²⁰ Under

²⁰ Given the significantly enhanced role that the Commission proposes for the Plan Processor, FINRA believes that the Commission must clarify the Plan Processor and Central Repository's regulatory status. FINRA has already organized FINRA CAT to ensure that, while it is a distinct subsidiary, it is nevertheless part of FINRA as an SRO and therefore an "SCI entity." See Securities Exchange Act Release No. 85764 (May 2, 2019), 84 FR 20173 (May 8, 2019) (Notice of Filing and Immediate

this modified SAW framework, the Plan Processor would still develop a revised CISP, as proposed, that addresses SAW environments in consultation with a formalized SWG. In addition, as proposed, the CISP would establish a uniform set of common security controls, policies, and procedures in accordance with NIST SP 800-53 that would apply to SAWs located within the Participants' own environments, recognizing the need for SAW-specific implementation contemplated by the Proposal.²¹ Moreover, as proposed, the Plan Processor would develop detailed design specifications for centralized security monitoring by the Plan Processor of each SAW account.²² In addition, FINRA would further support the Proposal's efforts to reinforce the application of common SAW security controls, policies, and procedures with independent audits required on a yearly basis, which would be available to the Commission through its regular oversight of the Participants.

FINRA believes this modified SAW framework alternative achieves the core benefits identified in the Proposal. Through reliance on central monitoring by the Plan

Effectiveness of File No. SR-FINRA-2019-015). However, under the Proposal, it is not clear whether the Commission would similarly require any other Plan Processor to be regulated similarly as an "SCI entity." In particular, the Commission states that the Central Repository itself is an SCI entity, although it is not clear how the Central Repository itself could be an SCI entity separate from the Plan Processor that is operating the Central Repository. *See* Proposal at 65996 n.54 (stating that "[t]he Central Repository, as a facility of each of the Participants, is an SCI entity...."). While, as noted, FINRA CAT is an SCI entity by virtue of its affiliation with an SRO, FINRA believes further Commission clarification is needed to ensure that any future Plan Processor is subject to appropriate regulation in light of its role within the national market system.

²¹ *See* Proposal at 66001 ("The Commission recognizes, however, that common implementation will likely not be feasible for all of the NIST SP 800-53 security controls, policies, and procedures required by the CISP. Accordingly, proposed Section 6.13(a)(ii)(B) would permit the security controls, policies, and procedures established by the CISP to indicate that implementation of NIST SP 800-53 security controls, policies, and procedures required by the CISP may be done in a SAW-specific way and by either the Plan Processor or each Participant.").

²² FINRA believes that a number of questions the Commission asks in the Proposal would best be resolved through the coordinated efforts of the Plan Processor and the SWG to develop the CISP and detailed design specifications. For example, the Proposal asks about a potential requirement that the CAT System use dedicated cloud hosts that are physically isolated from a hardware perspective. *See* Proposal at 66049 q.164. FINRA believes such a requirement is neither feasible nor necessary to enhance security. By allowing for coordinated development of the CISP and detailed design specifications, FINRA believes input from the appropriate security and subject matter experts will achieve the right balance of security and feasibility.

Processor and independent security assessments, the modified SAW framework would establish common security controls that would further be subject to independent review and verification. FINRA notes that its modified SAW framework alternative is largely grounded in elements already present in the Proposal. Specifically, a central-monitoring SAW framework would operate similar to the non-SAW exception process laid out in the Proposal. And it would further leverage, rather than discard, the substantial efforts already underway to implement the current SAW requirements that have been developed by the Participants and FINRA CAT and approved by the CAT Operating Committee. However, given the risks that would result from central SAW ownership, FINRA believes a central-monitoring framework is better suited as the primary rule, rather than framed as an “exception.” In addition, based on the controls that would remain in place in a central monitoring framework, FINRA believes that a Participant’s environment should not be characterized as “non-SAW” simply because it is not centrally owned within the CAT System. Under FINRA’s recommended alternative, CAT Data environments would in fact be secure analytical workspaces, subject to central monitoring according to common security controls and independent assessment, and FINRA believes the Proposal unnecessarily undermines public confidence in the security of such environments by labeling them as “non-SAW.”

C. Required Modifications to the Non-SAW Exception Process if the Commission Adopts its Proposed Centrally-Owned SAW Framework Rather Than FINRA’s Recommended Central-Monitoring Alternative

For the reasons explained above, FINRA believes its recommended central-monitoring SAW alternative achieves the intended benefits of the Commission’s Proposal without imposing undue regulatory risk and cost. In line with this discussion, FINRA believes it is important for the Commission to recognize that if it were to adopt the centrally-owned SAW framework laid out in the Proposal, FINRA would need to rely on the Proposal’s non-SAW exception process to continue its regulatory operations in the manner best designed to meet its obligations under the Exchange Act. In that case, however, FINRA believes certain changes to the exception process are needed to minimize the risk of regulatory disruption without diminishing any security controls or protections.²³

First, the Proposal would require any Participant that requests a non-SAW exception to provide an application package that contains extensive material to the Plan Processor’s CISO, the CCO, members of the SWG, and Commission observers of the SWG. FINRA believes that such an application package likely will include sensitive security information, as well as protected intellectual property, concerning a Participant’s

²³ In addition to the changes to the non-SAW exception process discussed in this section, FINRA also believes the Commission would need to reconsider the ability to access Customer and Identifying Systems from non-SAW environments, as discussed further below, to avoid compromising FINRA’s ability to use CAT Data as needed to support its regulatory programs.

environment that is not appropriate to share with representatives of other Participants through the SWG. Accordingly, Participants should be able to designate portions of the application package, or their notifications of material systems changes, as confidential for review only by the Plan Processor CISO and CCO and Commission staff. For similar security and confidentiality reasons, FINRA believes that the SWG should not be expanded formally to include other parties. While FINRA appreciates the value that the Advisory Committee and industry security experts can offer, FINRA believes that such expertise would more appropriately be provided upon invite through targeted working groups or subcommittees, where potential exposure to sensitive information could be more carefully managed.

Second, to avoid the potential for unnecessary and costly disruptions to market supervision, exceptions should not be formally reconsidered each year. Rather, the Commission could still require a new independent security assessment to be provided each year, which the CISO and CCO could act on if necessary and appropriate. This would ensure that there is still regular and consistent reevaluation of the security of non-SAW environments, while limiting the risk of unnecessary regulatory disruption and uncertainty.

Third, if the Commission adopts its proposed framework where the CISO and CCO are vested with significant authority to deny, terminate, or revoke an exception for the Participants that formed CAT LLC, to which the CISO and CCO owe fiduciary duties, it is critical that the Commission provides a clear, effective process for Participants to appeal such a decision.²⁴ FINRA appreciates that the Proposal already appears intended to avoid such an outcome by requiring the CISO and CCO to provide Participants with detailed written explanation of deficiencies that Participants could remedy. However, given the impact that a denial, termination, or revocation could have on a Participant's regulatory operations—and, therefore, market integrity—FINRA believes the Commission must establish a process with more clarity and safeguards. For example, the Proposal should not confer authority on the CISO and CCO to terminate or revoke an exception at will, nor

²⁴ FINRA notes that its recommended central-monitoring alternative does not contemplate a formal approval process for SAW usage. As noted in this paragraph, FINRA believes that vesting formal approval and disapproval authority in the Plan Processor, CISO, or CCO creates inherent conflicts that jeopardize the carefully constructed—and Commission approved—CAT NMS Plan governance structure. However, FINRA recognizes that even under its recommended alternative, there could be instances where the Plan Processor, CISO, or CCO identify deficiencies in a Participant's centrally-monitored SAW environment. FINRA believes such cases will likely be avoided by collective development of a CISP and common security controls, and to the extent they arise, resolved through discussion and mutual agreement. Nevertheless, if the Commission were to adopt FINRA's recommended alternative and impose oversight or enforcement obligations on the Plan Processor, CISO, or CCO, FINRA believes a formal appeal process would be needed in that case as well.

should there be authority to limit a transition period following a revocation decision where doing so would disrupt critical regulatory functions. The Commission must further ensure that it, not the Operating Committee, is the decisionmaker in any appeal process. Simply put, given the implications for overall market integrity, the need for clear and consistent standards, and potential competitive implications, it is not appropriate for the Commission to delegate to a majority of the Operating Committee the authority to review a decision that can significantly disrupt a Participant's operations, impose material costs, and threaten market integrity. Given the importance of any decision to deny, terminate, or revoke a non-SAW exception, the Commission must establish a clear path for timely Commission review and final Commission action.²⁵

D. Reasonable Implementation Periods for Any New SAW Framework

Finally, any new framework that the Commission adopts must include a reasonable implementation period to avoid regulatory disruption. It is not clear what the Commission used as a basis for its proposed implementation period of 180 days to be fully compliant with an entirely new SAW framework. In FINRA's experience, 180 days is not nearly enough time to make the extensive systems changes that would be required to migrate systems and data to a new centrally-owned SAW account, nor is it enough time to fully comply with the non-SAW exception process.

For one point of reference, FINRA has scheduled another six months to fully implement the current voluntary SAW concept—which the Commission now proposes to enhance with significant additional requirements—across all of FINRA's environments that use CAT Data. To fully migrate to the new centrally-owned SAW framework proposed by the SEC, FINRA believes such a dramatic undertaking would require at least 12-18 months of development work, which could only begin after requirements and specifications are finalized.²⁶ Alternatively, to prepare the extensive application materials required for the proposed non-SAW exception process, which must include an independent third party security assessment, FINRA believes it would reasonably take at least three months, rather than the 30 days allowed by the Proposal following completion of the CISP

²⁵ FINRA recognizes that there may already be existing methods to appeal such determinations, for example under Rule 608(d) of SEC Regulation NMS. However, FINRA believes a more definite appeal standard, process, and timeline are needed here given the potential impact such determinations could have on the regulatory programs that support market integrity and investor protections.

²⁶ FINRA's initial estimate of a 12- to 18-month period for it to implement the requirements and specifications of a centrally-owned SAW framework—once those requirements and specifications are complete—is based on the same assumptions discussed above with respect to implementation costs. Accordingly, this estimate is similarly uncertain, and changes to FINRA's assumptions would materially increase the time needed for implementation.

and SAW design specifications.²⁷ Importantly, FINRA notes that because its recommended central-monitoring alternative could leverage existing efforts, it therefore could be implemented far more efficiently.²⁸

While FINRA supports efforts to strengthen the SAW framework in service of enhanced CAT Data security, FINRA urges the Commission to engage in further dialogue to identify a feasible timeline for any new SAW framework it adopts. FINRA believes such dialogue will help the Commission advance the goals of the Proposal in a timely manner without jeopardizing the ongoing regulatory efforts needed to ensure market integrity and investor protection. And critically, FINRA notes that there is already a robust CAT security program in place—which is subject to Commission oversight and includes FINRA’s current SAW development work—that provide standing CAT safeguards during any implementation period.

III. Support for Customer and Account Provisions and Request for Additional Clarification

FINRA is broadly supportive of the Proposal’s approach to Customer and Account Attributes. As an initial matter, FINRA supports the Commission’s efforts to codify the revised approach to Customer and Account Attribute reporting by formalizing in the Plan the Personally Identifying Information (“PII”) Exemption Order. FINRA has long supported efforts to reduce the amount of sensitive data stored within the CAT, and FINRA appreciates the Proposal’s clarification that, under the PII Exemption Order, there will no longer be “PII” reported to CAT.²⁹

FINRA also supports the Proposal’s efforts to define a workflow for programmatic access to the CAT’s Customer Identifying Systems. Programmatic access is a necessary step towards reduced reliance on Electronic Blue Sheet (“EBS”) requests. As discussed

²⁷ See Proposal at 66053 (noting that Participants seeking a non-SAW exception “would have 30 days after the SAW design specifications have been provided to prepare their application materials for submission”). As with other cost and timing estimates, FINRA’s estimate for the three-month time period reasonably required to prepare an initial application package for a non-SAW exception is contingent on assumptions about future development of the CISP and design specifications. Changes to those assumptions could materially change this estimate.

²⁸ Based on FINRA’s efforts to implement the current voluntary SAW requirements, FINRA believes it likely could implement its recommended central-monitoring SAW alternative in a similar six-month period. However, FINRA’s implementation timeline would necessarily depend on, and begin later than, the substantial efforts that would first be required to develop a CISP and common security controls, and for FINRA CAT to design corresponding monitoring tools.

²⁹ See Proposal at 66017 (proposing to delete the term “PII” from the Plan).

above, FINRA relies on customer identifying information to surveil and investigate a range of activity, including insider trading, wash sales, fraudulent trading in furtherance of “pump and dump” schemes, prearranged trading, and offering manipulation. To perform this regulation effectively, FINRA must employ automated tools capable of performing complex data analysis on large data sets that cannot be replicated manually. The extent to which FINRA can use CAT Data in place of EBS data necessarily depends on FINRA’s ability to query, retrieve, and analyze customer identifying information and transaction data in the same manner it does today.³⁰

Accordingly, so that FINRA can better plan for its use of CAT Customer and Account Attributes and make efforts to reduce its use of EBS where appropriate, FINRA requests clarification on several elements of the programmatic workflow established in the Proposal. First, FINRA seeks confirmation that the Proposal’s examples of regulatory use cases where programmatic access may be approved are not exhaustive. As the Proposal recognizes, “certain regulatory inquiries based on the investigation of potential rule violations and surveillance patterns depend on more complex queries of Customer and Account Attributes and transactional CAT Data.”³¹ The Proposal then identifies several examples where such complex queries would be needed to identify and investigate potential misconduct, including investigations of trading abuses and other practices proscribed by Rule 10b-5 under the Exchange Act, Section 17(a) of the Securities Act, Rule 30(a) of Regulation SP and Rule 201 of Regulation S-ID, and Sections 206 and 207 of the Advisers Act. FINRA assumes these examples are not exhaustive, and that the Commission would approve programmatic access in other cases as well, for example to investigate potential violations of Regulation M, to perform market reconstruction after the occurrence of particular market events, or to perform surveillance of Customer and Account Attributes reporting compliance.

In addition to seeking clarity on the kinds of programmatic queries that the Commission would approve, FINRA also requests clarification of the proposed process for SEC approval of programmatic access. For example, under the Proposal, Participants must apply for programmatic authorization by providing, among other information, the regulatory purpose of the inquiry or set of inquiries requiring programmatic access. FINRA assumes that such approval would not be required on a query-by-query basis, given the Proposal’s reference to “inquiry or set of inquiries.” Given the Proposal’s timeline for

³⁰ FINRA also notes that, as discussed in the PII Exemption Order, regulators will still need to use EBS to obtain tax identifiers or account numbers now that such information will not be reported to CAT. Accordingly, while FINRA discusses here its support for efforts to reduce reliance on EBS through enhanced programmatic access to CAT’s Customer Identifying Systems, FINRA believes it is important to note that it will still need to issue EBS requests where tax identifiers and account numbers are essential in regulatory workflows.

³¹ See Proposal at 66031.

programmatic authorization—45 to 90 days—FINRA believes it is important to provide authorization at the rule or use-case level so that critical regulatory inquiries are not impaired or unduly delayed. This is again an area where FINRA believes further dialogue with Commission staff would be helpful to facilitate understanding of the necessary details of FINRA’s CAT Data usage.

Similarly, FINRA believes it is important for SEC staff to engage with FINRA so that FINRA fully understands the standards the Commission will use to approve or deny requests for programmatic access to CAT’s Customer Identifying Systems. Under the Proposal, the Commission shall approve programmatic access “if it finds that such access is generally consistent with one or more of the following standards: That such access is designed to prevent fraudulent and manipulative acts and practices; to promote just and equitable principles of trade; to foster cooperation and coordination with persons engaged in regulating, clearing, settling, processing information with respect to, and facilitating transactions in, securities; to remove impediments to and perfect the mechanism of a free and open market and a national market system; and, in general, to protect investors and the public interest.”³² FINRA appreciates the Commission’s goal to develop an approval standard that “allows for flexibility and the ability to tailor access to specific regulatory needs.” Based on FINRA’s unique regulatory role and experience, FINRA believes such flexibility is appropriate so that the Commission’s approval standards do not unduly limit legitimate regulatory use cases. FINRA would welcome further discussion with SEC staff on this point to ensure that expectations are aligned and that FINRA’s important regulatory efforts are not disrupted.

Finally, FINRA requests additional clarification of the ability to access CAT’s Customer Identifying Systems and to export the results of manual and programmatic queries from the CAT System. While FINRA recognizes the Commission’s efforts to impose heightened restrictions on access to and use of Customer and Account Attributes, FINRA believes the Commission must consider allowing access to this data from other specifically approved secure environments. In particular, FINRA believes the Commission should consider whether such access would be appropriate if a Participant can demonstrate that its secure environment is subject to the same security standards and controls as the CAT System—a requirement of non-SAW excepted environments under the Proposal—and if there would be comparable ability for the Plan Processor to monitor and capture information about such data access in the Participant’s environment. Where such conditions can be met, FINRA believes there is the potential for more efficient use of CAT Data in a secure manner that could also further reduce the necessity for FINRA’s surveillance programs to obtain transaction data and customer identifying information from EBS.

In addition, FINRA requests clarification of the ability to export the results of queries run in Customer Identifying Systems. For example, while the Proposal provides

³² *See id.* at 66032.

that Customer and Account Attributes may only be accessed and analyzed within SAWs, the Proposal allows that Customer and Account Attributes may be downloaded or extracted in the minimum amount required to achieve a specific surveillance or regulatory purpose.³³ Elsewhere in the Proposal, when discussing a parallel extraction limit required in the CISP, the Commission provides narrow examples of regulatory purposes that may warrant data extraction—specifically, responding to a court order or to some other regulatory or statutory mandate, to submit a matter to a disciplinary action committee, to file a complaint against a broker-dealer, or to refer an investigation or examination to other regulators like the Commission.³⁴ However, the Proposal does not appear to offer any examples of the specific surveillance purposes that could be served with data extracts, nor does it acknowledge other regulatory purposes that naturally result from surveillance efforts, for example where surveillance alerts result in further investigative or enforcement activity.

FINRA notes that several of its regulatory surveillance programs currently rely on programmatic review of transaction data combined with the results of EBS requests. If FINRA is unduly limited in its ability to access Customer Identifying Systems and export complex query results, FINRA would not be able to reduce its reliance on EBS while still performing the same effective regulation it provides today. As with other areas of the Proposal, FINRA believes it would be constructive to engage in further dialogue with Commission staff to obtain further detail on its regulatory use cases and the Proposal's potential impacts. Recognizing the Commission's goals of both enhancing effective regulation and facilitating the potential retirement of duplicative reporting systems, FINRA would welcome the opportunity to discuss this issue further with Commission staff.

IV. Support for Restrictions on Regulatory Use of CAT Data and Request for Additional Clarification

FINRA supports the Commission's efforts to limit the use of CAT Data to regulatory purposes only. FINRA recognizes that successful CAT implementation necessarily depends on the investing public's confidence that data reported to CAT will remain secure and appropriately confidential. And FINRA believes that the Proposal would help bolster public confidence by providing clear guidance that all data reported to CAT will be used only to support the regulatory efforts of SROs' "Regulatory Staff."

In its role as a not-for-profit national securities association, FINRA will only use CAT Data to achieve its mission of investor protection and market integrity. FINRA appreciates the Proposal's recognition of FINRA's unique structure, given that it maintains

³³ *See id.* at 66040 (discussing proposed Section 6.5(g)(i)(B) and stating that the requirement to limit extracts to the minimum amount of CAT Data necessary to achieve surveillance or regulatory purposes "would apply to all CAT Data, including transactional data and Customer and Account Attributes).

³⁴ *See id.* at 65998 (discussing proposed Section 6.13(a)(i)(C)).

“Regulatory Staff” in different departments and reporting lines throughout its organization.³⁵ FINRA further appreciates the Proposal’s acknowledgment that non-Regulatory Staff, whether in technology or operations, are necessary to facilitate Regulatory Staff’s access to and use of CAT Data.³⁶ In addition, given the regulatory nature of services that FINRA provides to other SROs pursuant to RSAs, FINRA believes the Proposal sets forth a workable approach to defining “Regulatory Staff” in such cases.

To help FINRA effectively implement appropriate CAT Data confidentiality policies, FINRA requests further clarification of the use of CAT Data in certain situations. The definition of CAT Data is broad, including “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.”³⁷ As the Proposal suggests, even aggregate or summary information derived from CAT Data that is used, for example, to brief a Participant’s executives or directors, may itself be considered CAT Data and therefore subject to access, handling, and use restrictions.³⁸ However, the Proposal also suggests that

³⁵ As the Commission correctly states, FINRA does not have a Chief Regulatory Officer and accordingly would designate multiple Executive Vice Presidents who lead departments of “Regulatory Staff.”

³⁶ With respect to access to CAT Data by operations staff to facilitate Regulatory Staff’s access to and usage of CAT Data, FINRA requests confirmation that operations staff may access or receive CAT Data solely to facilitate regulatory transaction fee billing, subject to affidavit, training, and other applicable requirements. CAT Data would facilitate the efforts of operations staff in FINRA’s Finance Department to more efficiently implement regulatory transaction fees, which serve to advance the regulatory purposes of FINRA and the Commission.

In addition, in response to a question posed in the Proposal, FINRA does not believe that a U.S. citizenship requirement is needed for administrators or other staff with access to the CAT System or the Central Repository. *See* Proposal at 66047 q. 157. FINRA notes that its prospective employees and contractors are already subject to background checks, including fingerprinting, to identify issues that would preclude employment. With these policies in place, coupled with the Proposal’s limitations on Regulatory Staff, FINRA believes there is no added benefit of a citizenship restriction, which poses various complications and would be both over- and under-inclusive for purposes of evaluating potential security threats associated with a person’s employment.

³⁷ *See* Proposal at 65591 n.4 (citing CAT NMS Plan, Section 1.1).

³⁸ *See id.* at 66039.

CAT Data may be used in public rule filings, provided such rule filings serve only a regulatory purpose.³⁹

Consistent with these provisions of the Proposal and the Plan, FINRA requests additional guidance on when CAT Data may be considered non-confidential and appropriately shared externally or publicly. For example, FINRA assumes that the use of aggregate or summary statistics in a public rule filing, even if such information is derived from CAT Data and therefore itself CAT Data, would be permissible where the information does not reveal anything confidential about the parties that reported the data to CAT. Similarly, FINRA routinely shares aggregate market information with member firms in report cards to facilitate those firms' compliance efforts, and it assumes it may continue to do so with aggregate, non-confidential CAT Data.⁴⁰ In addition, like the Commission, FINRA may include a description of market activity in public disciplinary complaints or settlement documents, where an expectation of confidentiality is not customary or reasonable.⁴¹ While FINRA believes these and similar use cases appropriately may be authorized by the confidentiality policies required under the Plan, confirmation or further guidance from the Commission would assist FINRA's efforts to develop its confidentiality policies in a manner that supports its regulatory mission.

FINRA also requests additional guidance on appropriate controls in certain cases where confidential CAT Data is used internally by FINRA's Regulatory Staff. As noted above, the Proposal discusses the controls that the Commission expects where briefing materials based on CAT Data are provided to executives or directors who are not otherwise considered to be Regulatory Staff.⁴² This discussion raises questions regarding other similar cases where briefing materials are provided to FINRA staff that do qualify as

³⁹ *See id.* at 66045.

⁴⁰ FINRA notes that report cards may also contain detailed data about the firm's own activity; while such information may be confidential, FINRA assumes it is permissible to share CAT Data with the reporting firm because confidentiality would be still be preserved in that case.

⁴¹ Relatedly, FINRA may need to share CAT Data concerning one firm with another firm in the regular course of an examination, investigation, or enforcement matter. Although such CAT Data may remain confidential at that stage, FINRA believes it is essential not to unduly restrict FINRA's customary and accepted regulatory practices, which would subvert the purpose of the CAT.

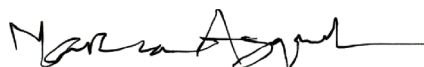
⁴² The Proposal notes that, where such briefing materials are provided to executives or directors who are not otherwise considered to be Regulatory Staff, documented approval of the regulatory need for such information sharing is required by a Chief Regulatory Officer (or similarly designated head(s) of regulation). The Proposal notes further that such access to CAT Data by non-Regulatory Staff would be subject to annual examination.

Regulatory Staff in the regular course of FINRA's regulatory operations. For example, based on its longstanding regulatory experience, FINRA anticipates that CAT Data will need to be presented in excerpt or summary form in memoranda that refer matters internally for consideration of further regulatory inquiry or enforcement. It would be difficult to maintain a full technical audit log of all such CAT Data movement.⁴³ However, FINRA believes that CAT Data shared in this manner necessarily will be limited by the memorandum format in which it is shared and therefore poses less risk of data leakage and misuse. Accordingly, FINRA believes reasonable data confidentiality policies may require such memoranda to be labeled as containing CAT Data, particularly regarding Regulatory Staff subject to training and affidavit requirements. While such use of CAT Data is difficult to subject to systemic logging, FINRA believes it can reasonably be subject to testing and review during the proposed annual examinations of confidentiality policies. FINRA believes it would be helpful for the Commission to confirm FINRA's view of appropriate controls in these kinds of cases of internal information sharing, so that FINRA may continue its natural regulatory efforts which support important investigative and enforcement activity.

V. Conclusion

FINRA thanks the Commission for its attention to FINRA's comments on the Proposal and looks forward to continued engagement with Commission staff on these important regulatory matters. If you have any questions or would like to further discuss FINRA's views and comments, please contact Jon Kroeper, Executive Vice President, Quality of Markets, FINRA, at (████████████████████) or Stephanie Dumont, Senior Vice President and Director of Capital Markets Policy, FINRA, at (████████████████████).

Sincerely,



Marcia E. Asquith
Executive Vice President,
Board and External Relations

⁴³ See Proposal at 66044 q.135.