Press Release

SEC Proposes Data Security Enhancements to the CAT NMS Plan

FOR IMMEDIATE RELEASE
2020-189

Washington D.C., Aug. 21, 2020 — The Securities and Exchange Commission today proposed amendments to the national market system plan governing the Consolidated Audit Trail (the "CAT NMS Plan") to bolster the Consolidated Audit Trail's ("CAT") data security. While the CAT NMS Plan currently sets forth a number of requirements regarding the security and confidentiality of CAT data, the proposed amendments to the CAT NMS Plan are the latest SEC action to limit the scope of sensitive information required to be collected by CAT and enhance the security of the CAT and the protections afforded to CAT data.

"Data security is an essential pillar of the CAT," said SEC Chairman Jay Clayton. "The requirements outlined in the proposal, including requiring the removal of sensitive PII, are designed to both (1) significantly reduce the amount of sensitive data collected without affecting the operational effectiveness of the CAT and (2) provide market participants with greater certainty regarding how CAT data will be protected and used. We will continue to evaluate these matters, including to address changes in risks and other matters, as implementation and operation of the CAT continues."

The public comment period will begin following publication on SEC.gov and remain open for 45 days after publication in the Federal Register.

* * *

Fact Sheet

Action
Today, the Commission voted to propose amendments to the CAT NMS Plan that are designed to enhance the security of the CAT through increased security requirements as well as limiting the scope of sensitive information required to be collected by the CAT.

Comprehensive Information Security Program
The proposed amendments would explicitly define the scope of the CAT's information security program by adding the term "Comprehensive Information Security Program" (the "CISP") to set forth all elements of the information security program, inclusive of the proposed Secure Analytical Workspaces.

Security Working Group
The proposed amendments would require the permanent establishment of a 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 self-regulatory organization that is a participant to the CAT NMS Plan (the "Participants"). The CAT CISO and the Operating Committee may invite other parties to attend specific meetings.

Secure Analytical Workspaces
The proposed amendments would define a Secure Analytical Workspace ("SAW") as an analytic environment account that is part of the CAT system, and subject to the CISP, where CAT data is accessed and analyzed. The proposed amendments would further require the CISP to establish data access and extraction policies. However, the proposed amendments would explicitly state that each Participant would be allowed to provide and use its own choice of software, hardware configurations, and additional data within its SAW, so long as such activities otherwise comply with the CISP.

The proposed amendments would require Participants to use their SAWs for analyzing CAT data accessed through user-defined direct query and bulk extract tools and for any customer and account data. Participants may only

extract from SAWs the minimum amount of CAT Data necessary to achieve a specific surveillance or regulatory purpose. The proposed amendments also set forth a process by which Participants may be granted an exception from using the SAW related to data accessed via user-defined direct query and bulk extract tools.

Online Targeted Query Tool and Logging of Access and Extraction
The proposed amendments would limit the maximum amount of records that regulators can download using an online targeted query tool. The proposed amendments would also enhance logging requirements by requiring logging of extraction of CAT data.

CAT Customer and Account Attributes (Removing Sensitive Personally Identifiable Information)
The proposed amendments would modify the Customer-ID creation process and reporting requirements in accordance with the exemptive order issued by the Commission on March 17, 2020. 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.

Customer Identifying Systems Workflow
The proposed amendments define the workflow for accessing customer and account attributes and establish restrictions governing such access. As described above, Customer Identifying Systems, which contain customer and account attributes, would have to be accessed through a Participant's SAW. Only Regulatory Staff may access Customer Identifying Systems and such access would have to follow role based access control ("RBAC") and the "least privileged" practice of limiting access to Customer Identifying Systems and customer and account attributes as much as possible. All queries of Customer Identifying Systems would have to be based on a "need to know" the data in the Customer Identifying Systems, and queries must be designed such that query results would contain only the customer and account attributes that Regulatory Staff reasonably believes will achieve the regulatory purpose of the inquiry or set of inquiries.

Access to Customer Identifying Systems would be limited to two types of access: manual access and programmatic access. For manual access, the proposed amendments generally provide that Regulatory Staff must have identified a Customer(s) of regulatory interest through their own regulatory efforts before they may use manual access to obtain additional information regarding such Customer(s). To use programmatic access, authorization would have to be requested and approved by the Commission pursuant to the process described in the proposed amendments, and Participants approved for such access may programmatically query the Customer Identifying Systems.

Participants' Data Confidentiality Policies and Regulator Access to CAT Data
The proposed amendments would require the Participants to establish, maintain, enforce and publish identical written data confidentiality policies. Each Participant would establish, maintain and enforce 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 proposed amendments would define the term "Regulatory Staff" 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. 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.

The proposed amendments 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).

Secure Connectivity and Data Storage
In addition to requiring connectivity to CAT infrastructure in a manner consistent with current implementation, the proposed amendments would require the Plan Processor to implement "allow" listing, which would limit access to CAT only to those countries where CAT reporting or regulatory use is both necessary and expected. In addition, the

proposed amendments would require that data centers housing CAT systems must be physically located in the United States.

Breach Management Policies and Procedures
The proposed amendments would modify existing requirements related to breach management policies and procedures to explicitly require corrective actions and breach notifications to CAT Reporters be a part of the Plan Processor's cyber incident response plan, modeled after Regulation SCI obligations.

In addition to the security-related items above, the proposed amendments would, consistent with previously granted exemptive relief, explicitly require customer and account attributes to be reported for Firm Designated IDs that are submitted in allocation reports, as is required for Firm Designated IDs associated with the original receipt or origination of an order.

What's next?
The proposal will be published on SEC.gov and in the Federal Register. There will be a 45-day comment period following publication in the Federal Register.

This release has been updated to note the comment period will begin following publication on SEC.gov and remain open for 45 days after publication in the Federal Register.

###