The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 32735

September 2, 2020

SEC Proposes Amendments to CAT NMS Plan to Enhance Data Security

[32735]

September 2, 2020 TO: Chief Information Security Officer Committee
Equity Markets Advisory Committee
Technology Committee RE: SEC Proposes Amendments to CAT NMS Plan to Enhance Data Security

On August 21, the SEC proposed amendments to the existing national market system (NMS) plan for the consolidated audit trail (CAT) ("CAT NMS Plan" or "plan") that are intended to enhance the security and protections for CAT data. Comments on the amendments are due 45 days from the date of publication in the Federal Register. We summarize the amendments of interest to members below.

Comprehensive Information Security Program and Secure Analytical Workspaces

The proposed amendments would refine the scope and standards for CAT information security. The amended plan would include a definition of "Comprehensive Information Security Program" (CISP) that clarifies that the CAT NMS plan processor must apply the NIST SP 800-53 industry standard to personnel and information systems that support the CAT. The amendments would also require the plan's Operating Committee to establish a security working group that advises the plan processor's CISO and the plan's Operating Committee on CAT information security matters.[1]

The amended plan would also require the plan processor to create "Secure Analytical Workspaces" (SAWs) and provide plan participants with SAW accounts to access and analyze CAT data. Participants would be required to use the SAWs to access and analyze customer and account information, including to obtain large amounts of transaction data via user-defined direct query and bulk extraction tools.[2] The SAWs would have common security controls, policies and procedures that meet NIST SP 800-53 standards,[3] but a plan participant could provide and use its own compliant software, hardware configurations, and additional data within its SAW.

Online Targeted Query Tool and Logging of Data Access and Extraction

The amended plan would limit the maximum number of records that a plan participant's regulatory staff can download via an online targeted query tool to 200,000 records per

query. The SEC believes that this limit would still accommodate the type of targeted searches for which the tool was designed, but also prevent large-scale downloading outside of the SAW or approved non-SAW environment. The proposed download limit, however, would not limit the number of results that a user could view and analyze within the tool.

The amended plan would also require the logging of both access to and extraction of CAT data that occurs through the three types of data access methods: online targeted query tool, user-defined direct inquiries, and bulk extraction tools.

Customer Account and Customer Identifying Information

The amended plan would change industry member reporting requirements in a manner consistent with the SEC's March exemptive order, which has allowed industry members to avoid reporting certain sensitive personally identifiable information (PII), *i.e.*, ITINs/SSNs, dates of birth and account numbers.[4] As proposed, the plan would not require industry members to report PII, but instead report other customer account and identifying information, including the birth year of natural person customers ("Customer and Account Attributes")[5] and the industry member firm designated ID for each trading account associated with all customers ("Firm Designated ID").

Based on this change, the plan processor would need to adopt a two-step process for creating a unique Customer ID that transforms a customer's ITIN/SSN/EIN in the CAT Customer ID Subsystem (CCID Subsystem) and links that ID to relevant Customer and Account Attributes in a Customer and Account Information System (CAIS) (collectively, "Customer Identifying Systems").[6] The amended plan would also explicitly require that plan participants and the SEC be able to use the Customer ID to track allocations to any customer or group of customers over time, regardless of the brokerage account used to enter the order.[7]

The amended plan would maintain much of the existing data storage requirements for Customer and Account Attributes, such as separate storage from other transactional CAT data.

Participants' Data Confidentiality Policies

The amended plan would clarify and enhance current requirements related to participants' data confidentiality policies. A participant's policy would need to limit data extraction to a specific surveillance or regulatory purpose and limit access to identified individuals with designated roles; establish, maintain, and enforce usage restriction controls; and establish monitoring and testing protocols to assess compliance. While all participants would need to establish identical policies, they could adopt different procedures that reflect differing organizational structures and operations.

The amended plan, however, would also establish baseline procedural requirements in a participant's confidentiality policy, including (i) submission of the plan to the plan processor's CISO and CCO, and plan Operating Committee, for review and approval; (ii) public publication on the participant's website or the CAT NMS Plan website; and (ii) periodic review of the policy's effectiveness and prompt action to remedy any deficiencies. Further, a participant would be required to have an independent accountant to perform an annual compliance exam of its policy, with the results submitted to the SEC upon completion.

Access and Use of Data

The amended plan would clarify that CAT data access must be consistent with a participant's confidentiality policy, *e.g.*, limited to surveillance and regulatory purposes. Specifically, a participant's regulatory staff and the SEC must be performing regulatory functions when using the data, including for economic analysis, market structure analysis, market surveillance, investigations, and examinations; the data could not be used when it would serve both a surveillance or regulatory purpose and a commercial purpose. For example, a participant could not use CAT data to support a commercially-driven SRO rule filing such as a new order type.[8]

Further, the amended plan would specify that a participant's access to CAT data be based on a "least privileged" approach that is sufficient to achieve regulatory purposes. For example, plan processor employees and contractors that develop and test Customer Identifying Systems could only use non-production data, or when needed, the oldest available production data.

Breach Management

The amended plan would further specify that the plan processor's cyber incident response plan must include taking appropriate corrective action that, at a minimum, mitigates potential harm to investors and market integrity, devotes adequate resources to remedy the breach as soon as reasonably practicable.[9] Further, a plan processor would be required to provide breach notifications to CAT reporting parties that it reasonably estimates may have been affected, as well as to plan participants and the SEC; this notification would need to occur after the process has a reasonable basis to conclude that a breach has occurred. A breach notification would need to include a summary description of the breach, including the corrective action taken and when the breach was or is expected to be resolved.

The plan processor, however, could delay such notification if it determines that dissemination of that information would likely compromise CAT security or an investigation of the breach. Further, the plan processor would not need to provide notification if it reasonably estimates that the breach would have no impact or de minimis impact on the processor's operations or on market participants.[10]

Firm Designated ID and Allocation Reports

The SEC proposes to require industry members to report Customer and Account Attributes for Firm Designated IDs that are submitted in connection with Allocation Reports. Allocation Reports, which are currently reported to the CAT, contain a unique Firm Designated ID assigned by the broker-dealer of a subaccount.[11] Without reporting identifying information for Firm Designated IDs, the SEC points out that the CAT cannot link subaccount holders to those that have the authority to trade on their behalf.[12]

Nhan Nguyen
Counsel, Securities Regulation

endnotes

[1] This working group would be composed of the plan processor's Chief Information

Security Officer (CISO) and the CISO (or deputy) of each plan participant, *i.e.*, the SROs.

[2] The amended plan, however, would also allow the plan processor (the CISO and CCO) to provide a pre-approved exception to SAW usage when accessing transactional data through user-defined direct query and bulk extraction tools. Non-SAW usage, however, would not be allowed to access Customer and Account Attribute data, as described further below.

[3] Common security controls, policies and procedures would be required for at least the following NIST SP 800-53 control families: audit and accountability, security assessment and authorization, configuration management, incident response, system and communications protection, and system and information integrity.

[4] In March, the SEC granted conditional exemptive relief from PII reporting requirements, which has facilitated an alternative approach to reporting CAT data that does not include PII. *See* Exchange Act Release No. 88393, 85 FR 16152 (Mar. 20, 2020).

[5] This information includes data elements found in the current definitions of "Customer Account Information" and Customer Identifying Information," excluding the PII to be eliminated. The new amended plan would replace those terms with two new terms: (i) "Customer Attributes," defined as "information of a sufficient detail to identify a [c]ustomer, including, but not limited to, (a) with respect to individuals: name, address, year of birth, individual's role in the account (*e.g.*, primary holder, joint holder, guardian, trustee, person with the power of attorney); and (b) with respect to legal entities: name, address, EIN, and Legal Entity Identifier ("LEI") or other comparable common entity identifier []"; and (ii) "Account Attributes," defined in part to "include, but not limited to, account type, customer type, date account opened, and large trade identifier (if applicable)."

[6] This two-step process involves (i) a first phase during which a customer's ITIN/SSN/EIN would be changed into a Transformed Value and submitted, along with other relevant information, to the CCID Subsystem; and (ii) a second phase where the CCID subsystem transforms the value to create a unique Customer ID for each customer. This ID would then be sent to the CAIS, which links the ID to corresponding Customer and Account Attributes.

[7] The current CAT NMS Plan requires that the plan participants and the SEC be able to use the unique Customer ID to track orders from any customer or group of customers, regardless of what brokerage account was used to enter the order.

[8] However, this prohibition would not prevent a participant from using the data that it reports to the CAT for permissible commercial purposes.

[9] The SEC notes that this language mirrors a similar requirement applicable to SCI entities for SCI events under Rule 1002 of Regulation SCI.

[10] The SEC notes that this proposed requirement mirrors Rule 1002(c) of Regulation SCI. The plan processor, however, would be required to document all information relevant to a breach that it considers de minimis.

[11] Prior to the approval of the CAT NMS Plan, the SEC provided exemptive relief permitting industry members to submit Allocation Reports (with Firm Designated IDs) in lieu of requiring the account number for any subaccount (to which an execution is allocated) to be reported. *See* Exchange Act Release No. 77265, 81 FR 11856 (Mar. 7, 2016). This approach was incorporated into the current CAT NMS Plan.

[12] The current NMS plan currently requires an industry member to report customer and account identifying information for firm designated IDs associated with the original receipt or origination of an order, but not for IDs contained within an Allocation Report.
