

## Part 2: Activities of the Broker-Dealer Operator and its Affiliates

### Item 2.7: Protection of Confidential Trading Information

Describe the written safeguards and written procedures to protect the confidential trading information of Subscribers to the NMS Stock ATS, including: i. written standards controlling employees of the ATS that trade for employees' accounts; and ii. written oversight procedures to ensure that the safeguards and procedures described above are implemented and followed.

The Operator maintains Written Supervisory Procedures ("WSPs") that govern the use of Confidential Trading Information.

The Operator classifies as Confidential Trading Information: orders and order handling instructions, executions, clearing reports, non-tape TRF reports, risk configurations, and Bidder Logic (as described in Part II Item 5). Intraday and historical data are both considered Confidential Trading Information. The commingling of data that would otherwise not be considered confidential with Confidential Trading Information (for example, application performance logs containing raw FIX message data) is also treated as Confidential Trading Information. Individuals with access to a system that stores or processes Confidential Trading Information are considered to have access to that information.

ACCESS TO AND USE OF CONFIDENTIAL TRADING INFORMATION: The Operator's activities as a broker-dealer are limited to operation of its alternative trading system. Operator employees operating the ATS may have access to Confidential Trading Information. A Series 24 registered supervisor ("ATS Supervisor") ensures the Operator restricts access to Confidential Trading Information to employees (and temporarily hired contractors, together with employees, "personnel") who are operating the ATS, those whose roles require access to such information for performing their duties, or those responsible for the Operator's compliance with Reg ATS and other applicable rules, as further described in Part II Item 7(c) below.

Operator personnel with access to Confidential Trading Information are only authorized to use such information as required by their job functions, and are prohibited from using such information for trading for their own accounts. They cannot disseminate such information to anyone not authorized to receive that information. The Operator requires all employees, including those with authorized access to Confidential Trading Information, to undergo annual compliance training that includes instruction and attestation relating to the protection of Confidential Trading Information.

The Operator performs at least quarterly reviews to confirm that those personnel with access to Confidential Trading Information continue to have a valid need to access such information, as described under KEY SECURITY CONTROLS below.

As covered more fully in the ATS's Subscriber Agreement, the Operator's personnel and certain third parties (such as accountants and lawyers) may receive a subscriber's confidential information, which may include Confidential Trading Information, in connection with performing services for the Operator or its subsidiaries or affiliates (e.g., auditing, development or surveillance). To the extent they may receive Confidential Trading Information, such persons will be legally bound by confidentiality obligations substantially similar to those that apply to the Operator under the Subscriber Agreement. Any such Information will not be shared until a third party has satisfactorily undergone a Third Party Risk Assessment (as described below under KEY SECURITY CONTROLS).

**KEY SECURITY CONTROLS:** The Operator employs a broad range of security controls to protect its trading systems and Confidential Trading Information. The principal controls are as follows:

- 1) **Centralized identity management:** The Operator maintains a central repository of user accounts for Operator personnel ("Internal Users"), which may include temporary contractors hired by the Operator as well as employees of the Operator. The Operator also maintains a central repository for all Subscribers and other External Users accessing the Portal described in Part II Item 5. Only an ATS Supervisor or a designee can establish new accounts for Internal Users or External Users. Internal Users may only access Confidential Trading Information if their accounts have been authorized, as discussed in the "Authorization" section in paragraph (3) below;
- 2) **Authentication:** The Operator requires the use of strong passwords meeting specified length and complexity requirements for all authenticated internal and external systems and services. Systems require multi-factor authentication whenever possible. Anti-brute-force mechanisms such as request throttling, IP whitelisting and blacklisting, account lockouts, and the use of cryptographic hashing help protect user credentials against both online and offline attacks;
- 3) **Authorization:** The Operator uses Role-based access control ("RBAC") to manage access to resources and systems for both Internal and External Users. In an RBAC process, categories of Roles are identified. Persons in particular Roles are given defined access to specific systems and resources, and thereby to specific categories of Confidential Trading Information. Accounts of specific Internal Users and External Users are granted Roles. Those Accounts can then only access a system or resource to the extent that their configured Roles allow the access. For example, an Internal User in the Operations area who requires routine access to cleared transaction information, but not to "live" orders, would be assigned an Account for which the Role was configured to deny access to live order information. A Subscriber External User would only have access to information related to its orders and transactions, and not to that of other Subscribers. The "principle of least privilege" dictates what Roles are appropriate for a given Account. The Operator's CCO or a designee of the CCO conducts periodic (at least quarterly) audits of Roles and their assignments to Accounts. These audits analyze the current and expected job functions of Operator personnel, the Roles configured for their Accounts, and

whether the systems, data, and other resources accessible through those Roles are necessary for those personnel to perform their job functions. As personnel responsibilities change, e.g. through assignments to new positions or due to systems or processes re-design, the CCO or designee would assess the (continued) need for those personnel to access specific kinds of Confidential Trading Information, and, as a result, the CCO or designee may require a change in Accounts or re-configuration of Roles;

- 4) Encryption: the Operator requires the use of strong encryption for data in transit over any untrusted network. Transmission of unencrypted data is not permissible unless a physical security model, e.g. a private cross connect between a Subscriber and an Operator trading system, provides comparable security guarantees. Media encryption protects Confidential Trading Information (as defined in Part II Item 7(d)) as part of the nightly archival process;
- 5) Physical Security: all production ATS trading systems are hosted in a SOC (System and Organization Controls) certified facility (described in Part II Item 6) which employs strong security controls, such as: surveillance, physical barriers, armed security, and multi-factor access controls. This facility maintains fully redundant HVAC and power systems to reduce the risk of outages and business interruptions. Control of production trading systems happens over a physically secured private network;
- 6) Change Management: The Operator employs a rigorous change management process for changes to all of its production systems, including the trading systems described in Part III and the Portal described in Part II Item 5 ("Production Systems"). Any proposed changes to Production Systems are analyzed by a designated "Change Team" for: software and/or configuration integrity; adherence to regulatory requirements and disclosures; impact on systems, operations, and practices; changes to External User-facing elements; and adherence to policies and procedures. These reviews include an assessment of the impact of the change on Confidential Trading Information, including how it is processed and stored, access to the information by Internal Users and External Users, and possible vulnerability to unauthorized access or misuse. The Change Team includes senior management of the Operator and ATS System, Business Development and Compliance managers;
- 7) Monitoring: the ATS uses a combination of proprietary and commercial software that monitors: a) trading system status, utilization, connectivity, and message rates; b) anomalies in trading data (orders, executions, reports, market data); and c) centrally aggregated system and application log data for anomalous events and unauthorized access to critical systems and systems containing Confidential Trading Information;
- 8) Incident Management: The Operator maintains a documented incident response process identifying steps to investigate and remediate security incidents, and a list of designated emergency contacts to alert upon detection of a security incident;

- 9) Third Party Risk Assessment: The Operator maintains a list of third-party suppliers with whom it conducts business. Before integrating any new third-party supplier, the Operator conducts a risk assessment that analyzes a) the type and classification of data that third party may access, and b) the potential threats to that data. For any third parties that have access to or may reasonably receive access to Confidential Trading Information, the risk assessment includes a thorough review of the third-party's security controls, business continuity controls, data protection and privacy practices, policies and procedures. These reviews focus on the ability of the third party to protect the confidentiality, availability, and integrity of Confidential Trading Information at each point where such information is stored or processed;

ATS EMPLOYEES' TRADING ACTIVITY: In accordance with FINRA Rule 3210 employees of the Operator must report to the CCO all personal investment accounts, as well as related accounts (those of immediate family members residing with the employee or to whom the employee provides material financial support, or other accounts the employee controls). These reports must be made to the CCO within 30 days of commencing employment or promptly upon opening a new account. Employees are strictly prohibited from trading on firm proprietary information, Confidential Trading Information, other confidential ATS External User information, and material non-public information ("MNPI"). The CCO surveils employee personal and related accounts for activity that may be indicative of possible abuses or violations of federal securities law, including those proscribing insider trading, which may include, as examples, excessive trading activity, activity that departs materially from typical activity in the account under review, or unusual trading activity in securities of a company with breaking news in the press. Operator employees operating the ATS may have access to External User orders and trading information; those and other employees described in Part II Item 7(d) may have access to information about Subscriber trading strategies and objectives. All Operator personnel are strictly prohibited from using any such information to their personal advantage. Annual compliance training includes materials and an attestation relating to employee trading activity, trading activity with regards to Confidential Trading Information, and identification, escalation and misuse of MNPI. The CCO reviews account statements received from broker-dealers where employees hold accounts on a monthly basis. Patterns of activity, as exemplified above, that may be indicative of insider trading or misuse of confidential data, including External User Confidential Trading Information, are subject to further scrutiny and escalation.

**Can a Subscriber consent to the disclosure of its confidential trading information to any Person (not including those employees of the NMS Stock ATS who are operating the system or responsible for its compliance with applicable rules)?**

Y

**If yes, explain how and under what conditions.**

A Subscriber or External User can consent to the disclosure of its confidential trading information by providing written or programmatic (through the Portal) permission to the operator. For example, a Subscriber or External User may submit a request to the Operator that the Operator share the Subscriber's or External User's Confidential Trading

Information with a third party Person to perform transaction cost analysis on their order and execution data, or to perform review of their Bidder Logic). The Operator may deny such a request if, for example, the disclosure conflicts with obligations the operator has to other Subscribers or External Users, or in other agreements. The operator must also have written confirmation from the Subscriber or External user of the type and classification of data that the Person may access. The Person will then be subject to all of the KEY SECURITY CONTROLS listed in Part II Item 7(a) with the exception of Third Party Risk Assessment.

**If yes to Item 7(b), can a Subscriber withdraw consent to the disclosure of its confidential trading information to any Person (not including those employees of the NMS Stock ATS who are operating the system or responsible for its compliance with applicable rules)?**

Y

**If yes, explain how and under what conditions.**

A Subscriber or External User can withdraw its previously provided consent and permission relating to the disclosure of its confidential trading information by written request to the operator.

**Provide a summary of the roles and responsibilities of any Persons that have access to confidential trading information, the confidential trading information that is accessible by them, and the basis for the access.**

Operator personnel responsible for the day-to-day operation of the ATS have access to Confidential Trading Information to the extent that their responsibilities require it, as provided by the RBAC process described in Part II Item 7(a). The following personnel are authorized to access Confidential Trading Information:

- 1) ATS Operations staff, who require access to Confidential Trading Information, e.g. for market surveillance, analysis, and customer support;
- 2) ATS Engineering staff, who require access to Confidential Trading Information, e.g. for development and support of ATS matching systems, and analysis of ATS matching performance as described in Part III Item 11;
- 3) Operator Supervisory and Compliance staff, who require routine access to Confidential Trading Information in summary form, e.g. for market surveillance and investigation of any errors or anomalies, and may require non-routine access to more detailed Confidential Trading Information in the investigation or analysis of particular events, activities or Users;
- 4) Sales staff, who require access to Confidential Trading Information in summary form, e.g. for analysis of ATS participation and liquidity properties. Individuals who do not have access to specific subsets of Confidential Trading Information, e.g. sales staff who are asked by a Subscriber for assistance in evaluating the efficacy of Bidder Logic used in constructing Expressive Orders, may request access from an ATS Supervisor or designee on an as-needed basis.

Deleted: all forms of

Deleted: historical order and execution data

Persons from third-party service providers as listed in Part II Item 6, may have access to Confidential Trading Information as necessary or appropriate in connection with their performance of services for OneChronos (for example: clearing, settlement, surveillance, fraud detection). Such access is permitted with limited scope, subject to the evaluation, legal agreement and audit procedures for third-party vendors described in Part II Item 7(a). As part of the quarterly audit process described under KEY SECURITY CONTROLS in Part II Item 7(a), the Operator will review the type and scope of access of third-party service providers to Confidential Trading Information. As part of the review, the Operator confirms those providers continue to have a valid reason to access such information.