This Form ATS-N amendment is being made to Part II Item 7a. New text is underlined and highlighted red. Deleted text is highlighted in red and strikethrough.

Item 7: **Protection of Confidential Trading Information**

a. 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.

A. General

Confidential trading information of participants of the Negotiation ATS may consist of:

* The identity of participants
* Orders (including match status) transmitted to the Negotiation ATS by or on behalf of a participant
* Trades executed in the Negotiation ATS by a participant.

In the response to Item 7.d. of this Part III, we describe the access to these categories of information by Liquidnet employees and on-site consultants.

In this response we address the following topics:

* External disclosure of identity of participants
* External disclosure of order and trading information
* Controls and procedures relating to access to and use and disclosure of trading information.

A. Identity of participants

LNI maintains the anonymity of all Members and customers.

B. Order and trading information

Liquidnet community trade advertising

Community trade advertising refers to any trade advertising that is limited to Members and customers. Examples of community trade advertising are advertising through Liquidnet 5, Liquidnet sales coverage, third-party EMSs and OMSs of Members and customers and Member and customer chat rooms. By default, Members and customers are opted-in to intra-day (including real-time) Liquidnet

community advertising of their trades. Through Liquidnet Transparency Controls, Members and customers can opt-out of intra-day Liquidnet community advertising of their trades.

Since only Members have access to Liquidnet 5, only Members can view trade advertising through Liquidnet 5, but Members and customers can view other types of community trade advertising. LNI may restrict a Member or customer from viewing community trade advertising based on the Members or customers Transparency Controls elections.

External trade advertising

External trade advertising refers to any trade advertising that is not limited to existing and prospective Liquidnet Members and customers. External trade advertising includes Bloomberg advertising. By default, Members and customers are opted-in to intra-day (including real-time) external advertising of their trades. Through Liquidnet Transparency Controls, Members and customers can opt-out of intra-day external advertising. After T+20, LNI can disclose executed trades to current and prospective Members and customers, regardless of whether the parties to the trade have opted out of external or community trade advertising.

Brokers and Liquidnet Capital Markets customers

By default, brokers that participate as customers cannot make elections through Liquidnet Transparency Controls and cannot opt-out from intra-day Liquidnet community and external advertising, subject to the following exception:

* Transition managers can make elections through Liquidnet Transparency Controls

LNI defaults Liquidnet Capital Markets (LCM) customers to intra-day community and external advertising. LCM customers cannot opt-out from intra-day community advertising. LCM customers can opt-out from intra-day external advertising. LCM customers do not have access to Liquidnet Transparency Controls. LCM customers can request either of these alternatives by contacting their trading coverage.

Additional detail on trade advertising

Upon request by a Member or customer, Liquidnet, in its sole discretion, can exclude the Members or customers trades from all Liquidnet trade advertising, including symbol-level and aggregated (not symbol-specific) advertising. This exclusion does not apply to any trade advertising that is required by the rules of a governmental or regulatory organization.

Reporting symbol-specific order and execution data to Members, customers, and prospects to attract block liquidity

Liquidnet sales and trading personnel can disclose symbol-specific execution data to Members, customers and prospective Members and customers if either of the following applies:

* External trade advertising is permitted for the trade based on the rules set forth above; or
* After T+20.

Disclosing symbol-specific execution data to existing Members and customers is permitted based on the rules for community trade advertising set forth above.

After T+20, sales and trading personnel can also disclose symbol-specific order information to Members, customers and prospective Members and customers. For example, sales and trading personnel may share algo order information to demonstrate the performance characteristics of Liquidnets algo strategies.

The purpose for this activity includes supporting existing participants, attracting additional liquidity from existing participants, and attracting additional participants to join the system and add to our liquidity pool.

Disclosure to 3rd-party vendors

LNI discloses execution data to certain 3rd-party vendors that provide services to the H2O ATS and are subject to contractual non-disclosure obligations. Examples of these vendors are LNIs clearing firm and a vendor that has developed software to display participant-specific risk management data in a graphical manner to Liquidnet support personnel.

Disclosure of aggregated data

LNI discloses certain aggregated trading data to participants and other third-parties. Aggregated data is not symbol-specific. Aggregated data may be broken out by one or more categories, including but not limited to: sector; index; and market cap (micro, small, mid and large).

Reports to participants relating to their own trading activity

LNI provides certain reports to participants relating to their own trading activity. For example, upon request, LNI provides to a participant on T+1 a report that includes all orders created by the participant the prior trading day and, for each order, whether at least one Member received a targeted invitation and whether there was a resulting execution. The purpose of these two reports is to assist participants in assessing the impact of Liquidnet functionality on execution quality.

C. Controls and procedures relating to trading information

Liquidnet has implemented various safeguards and procedures to protect the confidential trading information of participants in the Negotiation ATS. This response provides a summary of these procedures.

Access to internal applications

Liquidnet has implemented procedures for employees requesting access to applications that contain confidential participant information. An employee requesting access to an application that contains confidential participant information must request approval from his or her manager. If the manager approves the request, the manager must notify the gatekeeper for the application, as designated by Liquidnet. The gatekeeper manages access entitlements for the relevant application. The gatekeeper must notify Liquidnets Security and Risk Management (SRM) group. The manager must provide an explanation for any requested access. A manager cannot approve an access request unless the manager determines that: (i) the employee requires the requested access for the performance of his or her responsibilities on behalf of Liquidnet; (ii) providing the requested access will not adversely impact one or more Liquidnet participants; and (iii) Liquidnet has provided disclosure to its participants that would cover the requested access. SRM must sign-off on any new access entitlements. Compliance conducts oversight of this process. An employees access to an application continues until terminated by Liquidnet. SRM manages a process that involves the periodic review by each manager of the current access entitlements of the employees in the managers group to verify that existing authorizations are still appropriate.

Annual SSAE18 SOC2 and ISO 27001 assessments

Each year, Liquidnet engages an outside auditor to assess the suitability and implementation of Liquidnets information security controls. This assessment includes a review of Liquidnets processes and procedures for protecting the confidentiality of participant trading information. The report of this assessment (called an SSAE18 SOC2 assessment) is posted on the Liquidnet Member website and available to our participants at any time. Liquidnet also provides a copy of the assessment to participants upon request.

SSAE is the Statement on Standards for Attestation Engagements, which is overseen by The American Institute of Certified Public Accountants (AICPA) and more specifically the Auditing Standards Board (ASB). The SOC 2 report evaluates the business information systems that relate to security, availability, processing integrity, confidentiality and privacy.

Liquidnet also obtains an annual ISO 27001 certification. ISO 27001 is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organizations information risk management processes. According to the ISO 27001 documentation, ISO 27001 was developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system. Organizations can become ISO 27001 certified by undergoing a third-party assessment by an accredited auditor. Liquidnet engages an outside auditor to confirm that it has implemented information security compliant with ISO 27001. Liquidnets ISO 27001 certification is posted on the Liquidnet participant website and available to our participants at any time. Liquidnet also provides a copy of the certification to participants upon request.

Employee trading policies and review

~~Liquidnet requires~~
The Liquidnet Employee Trading Policy (the Policy) is designed to protect against trading on Member, Customer and Liquidity Partner confidential transaction information. The Policy is applicable to all Liquidnet employees ~~to report~~in the US, including those employees who possess FINRA-registered

licenses maintained by Liquidnet (Covered Persons). Covered Persons are permitted to maintain their personal brokerage accounts - and other related (i.e. IRA and ERISA) accounts, (Covered Accounts) with a third-party broker, subject to the requirements and restrictions set forth in the Policy. All Covered Persons are required to disclose and receive pre-approval of their Covered Accounts ~~to~~ from the Compliance Department~~. . Liquidnet prohibits employees from trading individual equities, subject to certain exceptions (for example, trading in an~~, and provide duplicate transaction confirmations, and if required, duplicate account ~~managed by a third-party; sale of stock acquired prior to employment by Liquidnet; and Direct Stock Purchase Plans). Liquidnet prohibits participation in initial public offerings as well as trading of individual stock options and other individual stock derivatives. Liquidnet permits trading in ETFs but requires a minimum holding period. Liquidnets~~statements. Prior to the establishment of a Covered Account with a third-party broker, a Covered Person is required to obtain approval from the Compliance Department. A Covered Person is permitted to buy and sell the following; equity securities, equity derivatives and ETFs in a Covered Account. Covered persons are prohibited from participating in Initial Public Offerings (IPOs).

The Liquidnet Compliance Department uses a third-party software product to facilitate disclosure and pre-approval of Covered Accounts and pre-clearance of transaction requests, and to assist in monitoring for ~~employee~~ compliance with ~~Liquidnets~~Liquidnet policies related to employee trading. The minimum holding period for Covered Persons is not required for transactions that have been pre-cleared by the Compliance Department. Liquidnet requires ~~employees~~Covered Persons to provide ~~confirmations and statements for their equity and ETF trading accounts. For~~ confirmations and statements ~~received electronically through the third-party software product,~~within the third-party software product ~~validates compliance with Liquidnets trading policies; for confirmations and statements received by mail, Liquidnets Compliance Department personnel monitor for compliance with Liquidnets trading policies.~~maintained by the Compliance Department.

Covered Employees who violate ~~Liquidnets~~Liquidnet's employee trading policies are subject to sanction, including potential termination of employment.

E-mail, IM and correspondence review

Liquidnet has policies for review of email, IM and other correspondence sent by registered Liquidnet employees. These reviews, which are conducted by Liquidnets business managers (with oversight by Compliance), include a review for any communications that could evidence misuse of customer information in violation of Liquidnet firm policy. Liquidnet maintains a record of all email, IM and other correspondence sent and received; these records are available for review by Liquidnet personnel as required in response to a regulatory inquiry or in connection with an internal review.

Supervisory process

Liquidnet supervisory personnel are required to certify on a monthly basis that any use of customer data within the supervisors business unit is in compliance with Liquidnet firm policy. Liquidnet personnel are only permitted to use customer data for the purpose of performing their respective business functions as described in the response to Item 7.d. of this Part II.

Trading Rules and Order Handling Q&A

The Liquidnet Trading Rules describe the various job functions within Liquidnet and the permitted access to and use of trading data by the employees performing each job function. Liquidnet employees are made aware of and required to comply with any limitations on access set forth in the Trading Rules. Such limitations are described in the response to Item 7.d. of this Part II. Supervisory personnel are required to monitor for compliance with these access limitations. These restrictions also are set forth in the Order Handling Q&A document, which Liquidnet updates on a quarterly basis and makes available to all participants.

Security and risk management department

Liquidnets Security and Risk Management (SRM) Department has responsibility for security and risk management functions at Liquidnet, which includes maintaining the security of customer trading information.

Pre-employment screening

Liquidnet conducts a pre-employment screening of employees for inconsistencies in application and resume information. After an offer is accepted, a criminal background screening may be conducted, subject to compliance with regulatory restrictions. All registered representatives must consent to a Pre-Registration Review.

Training and security awareness

SRM conducts onboarding and ongoing training for employees in Liquidnets information security policies and best practices.

System access controls

Liquidnet has instituted technological controls on access to trading information, including user name and password controls, secure remote access with two-factor authentication, access control lists on systems and networks, and network segmentation. These controls are evaluated on an annual basis by an external party, and included in an SSAE18 report and ISO 27001 certification, which are available to our participants and regulators.

Keycard controls and video surveillance

Liquidnets offices are equipped with keycard access controls and video surveillance. Liquidnets data centers are protected with a combination of keycard, biometric and video surveillance systems.

Monitoring of data transmission

All e-mail, web traffic and information copied to removable storage is monitored by a data leakage protection system, which provides alerts to the SRM Department should confidential information be detected in these communication channels.

Firewall and IDS protection

Liquidnets external network perimeters are protected by firewalls and intrusion detection systems. Liquidnet engages a third-party consultant to perform annual external network security assessments.

Liquidnet Transparency Controls

Liquidnet makes available to Members and buy-side customers a web-based system known as Liquidnet Transparency Controls. Liquidnet Transparency Controls allows Members and buy-side customers to view details about the liquidity sources with which they interact and the products and services they participate in that utilize their trading information. Members and buy-side customers use the tool to make elections relating to certain liquidity sources and products and services that access the participants trading information. See the response to Item 14 of Part III for additional detail regarding Liquidnet Transparency Controls.