**Part II: Activities of the Broker-Dealer Operator and its Affiliates**

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.

GENERAL BACKGROUND AND SCOPE OF CONFIDENTIAL INFORMATION. The Firm operates POSIT on a matching engine that runs on a standalone server in the NY5 Data Center. See Part I, Item 7; and Part III, Item 6(a). The POSIT matching engine communicates with shared systems to book trades, to report executed trades to the tape, to facilitate clearance and settlement, for financial reporting and billing, and to facilitate other post-trade processes. The Firm operates the Alert application on servers that are separate from the POSIT matching engine. These systems contain Confidential Information. See Part II, Item 6 for information on personnel that have access to Confidential Information.

AGGREGATED ANONYMOUS DATA. Data which has been aggregated and which does not identify any Subscribers is not Confidential Information ("Aggregated Anonymous Data"). The Firm publishes firm-wide aggregated anonymous execution data to market wide trade advertisement systems after the transaction has been reported to the consolidated tape. The data does not include any client identities but does include symbol level executed volumes. ~~The Firm includes POSIT Aggregated Anonymous Data in these reports at the end of day. The POSIT Aggregated Anonymous data is combined with the rest of the Firm's data when it is disseminated to these market-wide systems and is not separately identified or attributed to POSIT.~~ While the Firm does not consider this data to be Confidential Information, it ~~nonetheless permits Subscribers to opt out of having their data included~~does not include POSIT Aggregated Anonymous Data in these reports.

The Firm posts monthly statistics on its website and disseminates this data to Subscribers ("the Monthly POSIT and Alert Statistics"). The Monthly POSIT and Alert Statistics are available at https://www.virtu.com/about/transparency and provide aggregate and anonymous information about POSIT and Alert, including total volume; volume by sector; volume by market cap; fill size distribution; distribution of Alert block size, and distribution of executions at the bid, mid and offer. The Firm produces market commentary from time-to-time that discusses general market trends. The statistical data described in this paragraph can be used to produce market commentary. The Firm considers this data to be Aggregated Anonymous Data and not Confidential Information. The Firm does not permit Subscribers to opt out of having their data included in these reports.

SALES DATA. Sales Data is aggregated information about the products and services the Firm's clients use and includes the client's name, the product or service they use, aggregate executed volume, and revenues ("Sales Data"). Sales Data includes aggregated ATS data as described in

the preceding sentence. The Firm provides Sales Data to management personnel, Sales or Trading personnel, Relationship Management personnel and Alert Sales and Coverage personnel who are involved in handling relationships with the Firm's clients. Sales Data is provided for the purpose of allowing these personnel to keep abreast of the client's business activities to manage the client relationship and to cross sell the Firm's products and services to the client. The Firm does not consider Sales Data to be Confidential Information when distributed internally for the above described purposes. The Firm makes this information available in end of day reports and in sales systems (i.e., systems that support activities of Sales or Trading personnel**,** Relationship Management personnel and Alert Sales and Coverage personnel for the purposes described above) on T+1. The Firm prohibits personnel from disclosing Sales Data to third parties. The Firm does not permit Subscribers to opt out of having this data made available to personnel involved handling client relationships, as defined in Part II, Item 6(a).

PERSONNEL WITH ACCESS TO CONFIDENTIAL INFORMATION. The Firm does not have any personnel whose sole responsibility is for the operations of POSIT. The shared personnel discussed in response to Part II, Item 6(a), have access to Confidential Information.

SAFEGUARDS AND OVERSEEING CONFIDENTIAL INFORMATION. The Firm maintains written policies and procedures regarding use and protection of Confidential Information. Firm personnel are subject to its parent, Virtu Financial Inc.'s Code of Conduct and Employee Manual. Firm personnel are also subject to the Firm's Information Security Policy, Compliance Manual, and Written Supervisory Procedures.

These policies prohibit the personnel listed in Part II, Item 6(a), from sharing Confidential Information with other personnel who are not in one of these permitted categories or with any other person. The exception is that Compliance and Legal personnel may provide information to regulators in response to regulatory requests or to third parties pursuant to subpoena. Personnel who violate the Firm's policies concerning Confidential Information are subject to discipline, including termination of their employment. The Firm performs email reviews and employs data loss software as a means of safeguarding Confidential Information.

The Firm procedures require that personnel make requests for access to its systems through the Firm's access ticketing system and to receive approval from a supervisor prior to being granted access to any systems. The Firm's supervisory personnel grant access to systems on the premise that it is necessary to perform their duties and to carry out the purpose for which the information is provided to them. The supervisor responsible for POSIT and Alert approves requests for access to the POSIT matching engine and Alert application. The Firm only permits approved personnel in the categories described in Part II, Item 6(a), to have access to Confidential Information and only permits these personnel to access the systems and the Confidential Information contained therein using approved means of access and credentials. Supervisors do not grant access to Confidential Information. The Firm maintains a process that sends notifications to designated personnel to disable systems access for personnel who are no longer employed by the Firm. Supervisors are responsible for instructing the technology personnel to disable access when employees change roles. The Firm provides reports to the supervisors that show personnel with access to the POSIT matching engine and Alert application on a monthly basis. Supervisors review these reports to ensure that these personnel still require access to carry out responsibilities related to the ATS.

PERSONAL TRADING RESTRICTIONS. The Firm maintains employee trading policies that require personnel to disclose their own personal accounts and the accounts of close family members, that prohibit personnel from trading based on any client Confidential Information, that require personnel to pre-clear transactions and attest at the time of trade entry that they are not trading on Confidential Information, and that prescribe holding periods for securities purchases. The Firm conducts reviews of employee trading to determine whether trades were pre-cleared and whether holding periods were observed.

**Part III:** Manner of Operations

Item 14: Counter-Party Selection

a. Can orders or trading interest be designated to interact or not interact with certain orders or trading interest in the NMS Stock ATS (e.g., designated to execute against a specific Subscriber's orders or trading interest or prevent a Subscriber's order from executing against itself)?

Yes☐ No☐

If yes, explain the counter-party selection procedures, including how counter-parties can be selected, and whether the designations affect the interaction and priority of trading interest in the ATS.

POSIT:

Contra Participant Specific Blocking: Subscribers can request to block interaction with specific Subscribers within POSIT. Upon request, execution performance reports can be provided to Subscribers on their order flow, grouped by contra Subscriber, time in force, and peg instruction. Metrics included in the execution performance reports can include, but is not limited to, shares executed, average trade size, and stock price movement after the time of fill (mark outs). Contra Subscribers are anonymized in the execution performance reports. Upon receiving this information, a Subscriber can request which anonymized contra Subscribers to block interaction against, either in totality, or can specify specific contra Subscriber blocking by time in force and/or peg instructions. Once a Subscriber specifies a contra Subscriber block, that block will remain in effect until the Subscriber requests for that block to be removed. Subscribers can request Contra Participant Specific Blocking through their salesperson, who enter a ticket to make the request. Thereafter, an entry is made in a configuration file which takes effect in most cases on the next business day, but could take effect either the same day or greater than the next business day, depending upon the time of day the request is submitted.

Liquidity Guard: Liquidity Guard is an automated means where VAL prevents certain IOC and Peg orders from interacting with resting Peg orders. Stocks that are subject to the interaction restrictions of Liquidity Guard are those that have a historical bid offer spread that is greater than or equal to $0.03 per share or a trailing 21-day average daily volume that is less than or equal to 3 million shares. Liquidity Guard uses inputs including a stock's trailing intraday bid offer spread, historical bid offer spread, and volatility, to compute price bands where executions can take place

on a security basis. If a potential match of an incoming IOC or Peg order against a resting Peg order would occur at a price outside of the computed price bands for a particular stock, then the IOC or Peg order would be blocked from interacting against the resting Peg order. All Subscribers are subject to Liquidity Guard, but a Subscriber may elect to opt out of having their Peg orders subject to Liquidity Guard. Subscribers can request to opt out of Liquidity Guard through their sales person, who enter a ticket to make the request. Thereafter, an entry is made in a configuration file which takes effect in most cases on the next business day, but could take effect either the same day or greater than the next business day, depending upon the time of day the request is submitted. Subscribers are not provided with any information on when Liquidity Guard effected the interaction of their orders. Liquidity Guard is not employed in Alert.

Self-Match Prevention: Subscribers may provide instructions that will prevent orders from crossing if the resulting cross may result in a transaction with no change in beneficial ownership. Subscribers can request Self-Match Prevention through their salesperson, who enter a ticket to make the request. Thereafter, an entry is made in a configuration file which takes effect in most cases on the next business day, but could take effect either the same day or greater than the next business day, depending upon the time of day the request is submitted.

Further, Subscribers are able to block interaction against certain Virtu MPIDs. See the response to Part II, Item 3b for further detail.

Alert:

Participant Type Blocking: Electronic Participants can request to block interaction against Human Participants via a FIX tag, on an individual order basis. Human Participants can request to block interaction against Electronic Participants. This blocking instruction is supported at the session level.

Participant and Symbol Specific Blocking: Alert Sales and Coverage personnel can block certain participants in whole or at a symbol level. Alert Sales and Coverage personnel apply participant blocks in whole, or at a symbol level, on an intraday basis if a participant is having a technical issue. For example, if an Alert participant was duping messages repeatedly then the Alert Sales and Coverage personnel could introduce a temporary block until the issue was resolved. Alert Sales and Coverage personnel can lift this block once the participant verifies the technical issue has been resolved. Symbol level blocks are also applied on an automated basis between an Electronic Participant and a Human Participant if within a ~~three~~two-minute span, for a given symbol, ~~five~~three consecutive invitations to Firm Up between the two participants result in no trades, a ~~two~~one minute block will be applied between the two participants in the given symbol. After the two-minute blocking period, the block between the two participants will automatically be lifted in the given symbol. The three-minute time span begins at the time of when the first invitation is sent. Symbol level blocks do not carry over into the next trading day. Please see Part III, Item 9(a) for more detail on the POSIT Alert Conditional Order process.

Self-Match Prevention: Subscribers may provide instructions that will prevent orders from crossing if the resulting cross may result in a transaction with no change in beneficial ownership.