United States Securities and Exchange Commission
Washington, DC
FORM ATS-N
Intentional Misstatements or Omissions of Facts May Constitute Criminal Violations
See 18 U.S.C.1001 and 15 U.S.C. 78ff(a)

Type of Filing (select one)

☐ Initial Form ATS-N Rule	304(a)(1)(i)
☐ Material Amendment Rule	304(a)(2)(i)(A)
☒ Updating Amendment Rule	304(a)(2)(i)(B)
☐ Correcting Amendment Rule	304(a)(2)(i)(C)
☐ Order Display and Fair Access Amendment Rule	304(a)(2)(i)(D)

• Statement about the Form ATS-N Amendment pursuant to Instruction A.7(g) of this form:
This Updating Amendment amends Part II, Items 1(a) and 7(a) to update the names of the component groups of the Instinet, LLC trading desk. The changes herein apply to the Broker Dealer Operator and all Subscribers.

• Provide the EDGAR accession number for the Form ATS-N filing to be amended:
0000310607-20-000015

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

Item 1: Broker-Dealer Operator Trading Activities on the ATS

a. Are business units of the Broker-Dealer Operator permitted to enter or direct the entry of orders and trading interest (e.g., quotes, conditional orders, or indications of interest) into the NMS Stock ATS?

Yes ☒ *No* ☐

If yes, name and describe each type of business unit of the Broker-Dealer Operator that enters or directs the entry of orders and trading interest into the ATS (e.g., NMS Stock ATS, type of trading desks, market maker, sales or client desk) and, for each business unit, provide the applicable MPID and list the capacity of its orders and trading interest (e.g., principal, agency, riskless principal).

The ATS is owned and operated by Instinet, LLC ("ILLC" or the "Firm"), a broker-dealer registered with the Securities and Exchange Commission. The Firm's brokerage business takes place on a single trading desk. The component groups of ILLC's trading desk are: (1) Execution Trading; (2) Electronic Sales Trading; (3) International Sales Trading; (4) Program Sales Trading; (5) Cash and Hybrid Sales Trading; (6) Latency Sensitive Electronic Trading; (7) Event Driven Trading; and (8) Derivatives and Broker Dealer Execution. ~~(1) U.S. Institutional, U.S. Product & Derivative Sales; (2) U.S. Hybrid Sales~~

~~Trading; (3) Global Program & Execution Trading; (4) U.S. Electronic Sales Trading; (5) International & Broker Dealer Sales & Trading; and (6) Latency Sensitive Electronic Trading.~~ Component groups of the ILLC trading desk may submit trading interest to the ATS as agent or principal, although the desk primarily acts in an agency capacity. The ILLC trading specialist groups utilize the INCA MPID and, except as otherwise noted herein, trade on an agency basis.

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.

BACKGROUND AND SCOPE: The ATS system (e.g., matching engine and associated applications) (the "ATS Core) comprises standalone hardware and software applications that are maintained separately from ILLC's systems used to support its agency broker-dealer business (the "ILLC Core"). ILLC maintains policies and procedures designed to safeguard the confidential trading information of Subscribers as well as virtual barriers to prevent unauthorized access to such information.

ILLC's Core is the conduit through which firm-wide order information is processed (e.g., agency broker-dealer order and execution information). Indirect Subscriber orders routed to the ATS via an Instinet Trading Product pass through the ILLC Core. Direct Subscriber orders are routed to the ATS via dedicated FIX connections and do not pass through the ILLC Core in route to the ATS.

EMPLOYEES WITH ACCESS TO SUBSCRIBER CONFIDENTIAL TRADING INFORMATION: Instinet does not have any employees solely responsible for the ATS. The employees described in response to Part II, Item 6(a) have access to Subscriber confidential trading information. These employees are prohibited from sharing any Subscriber confidential trading information with persons not expressly permissioned to receive such information under Instinet policy, as described in Part II, Item 7(a) of this form.

SYSTEMS WITH ACCESS TO DIRECT SUBSCRIBER CONFIDENTIAL TRADING INFORMATION: ILLC Data messages are periodically written to a database for storage and retention (the "Core Database"). This information includes Direct and Indirect Subscriber order and execution information from both the ATS Core and the ILLC Core systems, as well as other ILLC data. Instinet maintains a Core Web Graphical User Interface ("Core Web GUI"), which allows a user to query the Core Database for the purposes of monitoring, reporting, and testing the Instinet systems and applications, including the ATS.

Access to the Core Database via the Core Web GUI is limited to personnel supporting the operations of the ILLC and ATS Cores and related databases and compliance supervisory personnel. Employees

responsible for operating the ATS Core include Operations and Technology Personnel and ETP Personnel whose responsibilities include the operation of the ATS. Members of the Liquidity Venues Team are permissioned to access Subscriber order and execution information. ATS data, including Direct and Indirect Subscriber order and execution information, is a subset of the data retained on the Core Web Database. ILLC personnel whose responsibilities include the operations of the ATS and related systems or its compliance with applicable rules, may be permissioned to access Subscriber order and execution information via the Core Web GUI. Other ILLC personnel may be permissioned for access to the Core Web GUI, but will be prevented from accessing subscriber confidential trading information. ILLC reviews and permissions employees for access to the Core Web GUI in accordance with the policies and procedures outlined in Part II, Item 7(a)(ii) below.

Physical access to Instinet's servers and databases is limited to employees responsible for operating the system and is generally further limited to employees performing necessary IT functions. Instinet servers and databases are housed in locked rooms requiring keycard access. Entry and exit is monitored via video surveillance. ILLC reviews and permissions employees for physical access to Instinet's servers and databases in accordance with the policies and procedures outlined in Part II, Item 7(a) (ii) below.

SYSTEMS WITH ACCESS TO INDIRECT SUBSCRIBER CONFIDENTIAL TRADING INFORMATION: The Newport OMS and Instinet Execution Experts can transmit Subscribers' confidential trading information to the extent orders are managed by the Newport OMS or routed through an Experts strategy. Data related to Indirect Subscriber orders managed by the Newport OMS or routed through an Experts strategy is accessible through certain GUIs that can disseminate information regarding the destination market center for a given order (e.g., the ATS) and whether a previously routed order was executed or cancelled.

Through the Newport OMS, Technology and ETP Personnel who support the Experts strategies or the OMS utilized may access real-time and post-trade Indirect Subscriber order and execution information routed or managed through the relevant strategy or OMS (Direct Subscriber order and execution information will not pass through an Instinet OMS or the Experts). Sales and Trading Personnel may also be permissioned, based on client coverage, to access real-time and post-trade order and execution via the Newport OMS. Note, certain members of the ~~U.S.~~ Electronic Sales Trading component group of the ILLC trading desk are considered client coverage for all clients utilizing the Experts algorithms.

Note, the information available to such support or trading personnel is provided by systems supporting the relevant strategy or OMS and does not include information regarding an order's priority or status in the ATS or another market center. Information regarding ATS orders and executions that do not relate to the relevant strategy or were not managed by the OMS is not transmitted by these systems.

SUBSCRIBER CONFIDENTIAL TRADING INFORMATION SAFEGUARDS:
ILLC requires permissioned logins to access Instinet Systems. Additionally, Instinet's global cyber security efforts, including measures to detect and prevent unauthorized access to Instinet systems,

apply to ILLC and its affiliates, including the operation of the ATS. Relevant Principals and Supervisors must approve employee access to Instinet systems, including the ATS and the applications with the ability to access Subscriber confidential trading information outlined above.

SEPARATION: ILLC has implemented physical and virtual information barriers to separate ATS data from other ILLC data and, in turn, separate personnel and systems with access to Subscriber confidential trading information from those not permitted to access such information.

ACCESS TO DIRECT SUBSCRIBER INFORMATION: Employees seeking to access the systems that may transmit or disseminate Direct Subscriber Information (see above section titled Systems with Access to Direct Subscriber Confidential Trading Information) must receive approval from the ATS Supervisor. In reviewing such requests, the ATS Supervisor considers factors including the employee's current role and whether the employee performs a function related to the operations of the ATS and related systems or its compliance with applicable rules that requires access to Direct Subscriber information. An employee's request for access may be denied if, based on the ATS Supervisor's review: (1) the employee's stated job function does not relate to the operations of the ATS and related systems or its compliance with applicable rules, (2) the employee has requested a type of permissioning (see below) that is too broad for the employee's stated job function, or (3) the employee can perform their stated duties without such access.

If an employee changes roles, the ATS Supervisor will adjust the employee's access to appropriately reflect the employee's new role. Based on this review, the ATS Supervisor or delegate may revoke, suspend, or modify access.

Decisions to approve access are subject to a periodic review pursuant to ILLC's Regulation ATS written supervisory procedures ("WSPs") described below. On a monthly basis, the ATS Operations Principal or delegate conducts a review to confirm the appropriateness of user access to Subscriber confidential trading information, including verification that users whose roles have changed and/or, employees who have been inactive, transferred or terminated have their permissioned access modified accordingly. Based on this review, the ATS Supervisor or delegate may revoke, suspend, or modify access.

ACCESS TO INDIRECT SUBSCRIBER INFORMATION: Employees seeking to access the systems that may transmit or disseminate Indirect Subscriber information (see above section entitled Systems with Access to Indirect Subscriber Confidential Trading Information) may be permissioned to do so on an as needed basis.

PERSONAL TRADING RESTRICTIONS: Instinet Incorporated maintains an Employee Investment Policy (the "EIP") which covers employees of all U.S. subsidiaries, and includes employees supporting the ATS. The EIP is designed to encourage long-term investments and prohibits employees from engaging in day-trading activities. Instinet prohibits all employees, including those with access to

Subscriber Confidential Trading Information, from trading based on non-public, or other confidential information.

The EIP requires employees to maintain EIP covered accounts at specified brokers that have agreed to provide Instinet daily trading information for employee personal accounts. EIP covered securities are subject to a 15-day holding period.

Prior to entering any trades in a personal account covered by the EIP, employees must enter a trade approval request via the Personal Trading Control Center ("PTCC") tool and receive an approval from both their supervisor and PTCC group. The PTCC tool requires the employee to certify that the employee: (1) is not in possession of any material non-public information concerning the security or commodity the employee proposes to buy or sell; (2) does not know of a pending customer trade nor of a pending research report in the security or commodity; (3) is not engaging in personal trading activity that violates Instinet's policies and procedures, including the Code of Ethics, or any duties owed to Instinet or its clients; (4) has reviewed Instinet's restricted list and the proposed transaction is not on the restricted list; (5) has confirmed that the proposed transaction meets the holding period requirement; (6) agrees that the proposed transaction must be effected on the same day on which approval is given; and (7) has confirmed that the proposed transaction(s) does not involve the purchase of an initial public offering (IPO) or any other type of new equity issue.

In approving or denying such a request, supervisors may review the employee's trades for any unusual activity, possible front-running customer trades or research, or conflicts with any of Instinet's businesses.

In addition, supervisors consider whether transactions are appropriate, given the employee's economic status and investment experience and whether the transactions are of such a frequency that they may distract the employee from his or her responsibilities at Instinet.

Separately, the Compliance Department reviews personal trades daily and consults with managers if irregularities are identified.

Generally, if an approval for an employee trade is given, it remains in force for the trading day in which it was received. Once an employee receives written confirmation approving a covered transaction, the employee may enter a trade in that symbol.

Employee supervisors review each employee's trading activity on a post trade basis and check for irregularities and potential red flags. In the event any irregularities or red flags are discovered, supervisors are to escalate the matter to Instinet management and the ILLC Chief Compliance Officer. Instinet, in its discretion, may take any action against an employee found to have violated the EIP, up to and including termination.

CONFIDENTIAL INFORMATION AND INSIDER TRADING: Instinet Incorporated maintains a policy regarding confidential information and insider trading which covers employees of all U.S. subsidiaries, including employees supporting the ATS.

Employees must not disclose any confidential information to anyone who is not authorized by Instinet to receive it pursuant to these policies and may not use such information, other than in the course of their employment and in connection with the performance of the duties for which access to such information has been granted. Accordingly, employees may not use confidential information to: (1) trade securities for their own accounts, accounts in which they have a direct or indirect beneficial interest, or accounts over which they can exercise control; or (2) advise relatives, friends, or other persons about possible securities transactions. Nor may employees authorize anyone else to disclose or use confidential information in a manner that would violate these prohibitions.

WRITTEN PROCEDURES: ILLC's Regulation ATS WSPs provide specific guidelines for the initial review and approval process, as well as the ongoing evaluation of, employee access to ATS data.

Prior to granting any employee access to Instinet's systems, including the ATS and the applications with the ability to access Subscriber confidential trading information must review and document each employee's level and type of access requested, the role and responsibilities of the employee, and the purpose for which access was requested.

On a monthly basis, employee access is reviewed to determine whether their level of access to Instinet's systems, including the ATS and the applications with the ability to access Subscriber confidential trading information remains appropriate. The ATS Supervisor must document each review and the changes made, if any, to employee access.

Periodically, the Internal Audit group reviews the ATS operations generally. Such reviews typically include testing the ATS WSPs, assessing the ATS Supervisor's review of employee access, and confirming that each review has been properly documented.