

United States Securities and Exchange Commission
Washington, DC
FORM ATS-N

Type of Filing:

- ☐ 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 Material Amendment to Form ATS-N for BlockCross provides for the addition of Amazon Web Services as a service provider in Part II, Items 6 and 7. This change applies to the Broker Dealer Operator and all Subscribers.

- Provide the EDGAR accession number for the Form ATS-N filing to be amended:

0000310607-21-000004

Part II: Activities of the Broker-Dealer Operator and its Affiliates**Item 6: Activities of Service Providers**

- a. *Does any employee of the Broker-Dealer Operator or its Affiliate that services both the operations of the NMS Stock ATS and any other business unit or any Affiliate of the Broker-Dealer Operator ("shared employee") have access to confidential trading information on the NMS Stock ATS?*

Yes ☒ No ☐ *If yes, identify the business unit, Affiliate, or both that the shared employee services, and provide a summary of the role and responsibilities of the shared employee at the ATS and the business unit, Affiliate, or both that the shared employee services.*

BACKGROUND AND SCOPE: Subscribers' confidential trading information includes Subscriber order and execution information and excludes post-execution transaction information of the type made public under reporting rules or regulations, or of an aggregated nature (e.g., aggregated and anonymous order and execution statistics aged at least one day (T+1) from the date of execution) to be Subscriber confidential information.

Instinet is an indirect wholly-owned subsidiary of Nomura Holdings Inc. ("NHI"). ILLC is a wholly-owned direct subsidiary of Instinet Holdings Incorporated ("IHI"). ILLC's affiliate, Instinet Group, LLC ("IGLLC"), is also a direct, wholly owned subsidiary of IHI. IHI is a wholly-owned direct subsidiary of Instinet Incorporated ("Instinet"). Certain personnel that provide services to the ATS are employed by IHI, IGLLC, or ILLC and certain compliance functions are outsourced to NHI ("Shared

Employees"). Instinet does not have any employees who are solely responsible for the ATS. Listed below are the Shared Employees that service the ATS, ILLC, or an ILLC affiliate and have access to Subscriber confidential trading information.

TECHNOLOGY PERSONNEL: Employees that provide information technology ("IT") support, IT development and strategy, tech management, and regulatory reporting services to the ATS (collectively "Technology Personnel"), also provide similar services to (i) ILLC's other business lines and (ii) some other subsidiaries of Instinet, including locally registered brokers Instinet Canada Limited, Instinet Canada Cross Limited, Instinet Europe Limited, Instinet Pacific Limited, Instinet Australia Limited, Instinet Germany GmbH, and Instinet Singapore Limited. For ILLC and the Instinet BD Affiliates, Technology Personnel are responsible for the operation, development, monitoring, and testing of various technology systems. For the ATS, certain groups of Technology Personnel are responsible for the operation, development, monitoring, and testing of the ATS's coding, network infrastructure, and software applications. In connection with the performance of their duties, Technology Personnel may access real-time and post-trade Subscriber order and execution information, including orders that were submitted to the ATS but were subsequently cancelled or did not otherwise receive an execution in the ATS. Separately, some Technology Personnel with direct physical access to ILLC servers and databases have the ability to access log files containing Subscriber order and execution information. Technology Personnel are employed by either ILLC, IHI, or IGLLC.

OPERATIONS AND COMPLIANCE PERSONNEL: Employees that provide customer support, finance, clearing and middle office support and compliance supervision to the ATS (collectively "Operations Personnel") also provide services to ILLC's other business lines and, as needed, certain Instinet BD Affiliates. Customer support personnel are responsible for addressing client inquiries related to connectivity to the ATS and client trading activity and can access real-time and post-trade Subscriber order and execution information in connection with executing their duties. Clearing, middle office support, and Finance are responsible for the clearance, settlement, and billing of transactions and can access post-trade Subscriber order and execution information, including orders that were submitted to the ATS but were subsequently cancelled or did not otherwise receive an execution in the ATS, in connection with executing their duties. Compliance personnel have a range of responsibilities including, but not limited to, responding to regulatory inquiries or performing internal audits of ILLC or its affiliates, including the ATS. Generally, compliance personnel may access post-trade Subscriber order and execution information, including orders that were submitted to the ATS but were subsequently cancelled or did not otherwise receive an execution in the ATS, in connection with executing their duties but may, when appropriate, be permissioned to access real-time Subscriber order and execution information. Operations Personnel are employed by either ILLC, IHI, or IGLLC.

ELECTRONIC TRADING PRODUCTS PERSONNEL: Employees that provide product development, customer support, and product sales support for the Instinet Trading Products (collectively "ETP Personnel") may also provide support to the ATS. Many ILLC clients access the ATS via an Instinet Trading Product. Accordingly, ETP Personnel may provide customer support to Indirect Subscribers as a result of the customer's use of an Instinet Trading Product as a means of

access to the ATS. For ILLC, ETP Personnel are responsible for the development, testing, and sales and technology support of the Instinet Trading Products as well as other components of the Instinet systems. For the ATS, ETP Personnel are responsible for the development, testing, and monitoring of the Instinet Trading Products' interaction with the ATS and for compiling data and analytics in response to requests from Subscribers. ETP Personnel may access real-time and post-trade Subscriber order and execution information, including orders that were submitted to the ATS but were subsequently cancelled or did not otherwise receive an execution in the ATS, to support the development, testing, and monitoring of the Instinet Trading Products and to respond to Subscriber requests for data or analytics. ETP Personnel are employed by either ILLC, IHI, or IGLLC.

U.S. LIQUIDITY VENUES TEAM: Employees that provide product strategy, customer support, and sales support for the Instinet ATSS (collectively "Liquidity Venues Personnel") also provide support for other ILLC businesses. For the ATS, Liquidity Venues Personnel provide customer support to Direct Subscribers. For ILLC, Liquidity Venues Personnel develop reports for use by internal groups in monitoring, developing, and enhancing ILLC's products and services. Liquidity Venues Personnel may access real-time and post-trade Subscriber order and execution information, including orders that were submitted to the ATS but were subsequently cancelled or did not otherwise receive an execution in the ATS, to support each Subscriber's use of the ATS and compile data and analytics in response to requests from Direct Subscribers.

SALES AND TRADING PERSONNEL: Trading desk personnel within the component groups identified in Part II, Item 1(a) (collectively, "Sales and Trading Personnel") are responsible for providing order routing and execution support to clients including addressing Subscriber inquiries regarding their orders routed to the ATS or other market centers. Sales and Trading Personnel may access real-time and post-trade Subscriber order and execution information, including orders that were submitted to the ATS but were subsequently cancelled or did not otherwise receive an execution in the ATS, in connection with executing their duties. Sales and Trading Personnel are permissioned for access to such information based on client coverage. The information that may be viewed includes the destination market center for a given order (e.g., the ATS) and whether a previously routed order was executed or cancelled. Sales and Trading Personnel are employed by ILLC.

- b. Does any entity, other than the Broker-Dealer Operator, support the services or functionalities of the NMS Stock ATS ("service provider") that are required to be explained in Part III of this form?***

Yes ☒ No ☐ If yes, both identify the service provider and provide a summary of the role and responsibilities of the service provider in response to the applicable Item number in Part III of this form, as required. List the applicable Item number here. If there are services or functionalities that are not applicable to Part III, identify the service provider, the services and functionalities, and also provide a summary of the role and responsibilities of the service provider here.

Pursuant to an Assignment of Intellectual Property between ILLC and IHI, IHI licenses to ILLC intellectual property employed by ILLC in connection with the operation of the ATS. Specifically, IHI licenses the ATS matching engine (see Part III Item 11), the functionality used to input and utilize market data (See Part III Item 23), and the systems and infrastructure providing connectivity to the ATS (See Part III Item 6). In addition, IHI develops and licenses certain algorithmic trading products to ILLC (See Part III Item 5).

Employees of IHI and IGLLC provide services to the ATS as detailed in Part II Item 6(a) above and Part II Item 7(d) below.

ILLC utilizes Broadridge Financial Solutions, Inc. systems and services for the purposes of recordkeeping, clearance and trade settlement processing. ILLC utilizes FIS for securities lending and WORM storage. CoreSite Realty Corporation hosts ILLC's primary data center in Secaucus, NJ. Rackspace U.S., hosts ILLC's secondary data center in Somerset, NJ.

ILLC utilizes Amazon Web Services, Inc. ("AWS") for cloud computing on the Platform as a Service (PaaS) model for data storage and retention.

c. If yes to Item 6(b), does the service provider, or any of its Affiliates, use the NMS Stock ATS services?

Yes ☐ No ☒ *If yes, identify the service provider, or the Affiliate as applicable, and the ATS services that the service provider or its Affiliates use.*

As stated in response to Part II Item 6(a), the Instinet BD Affiliates are wholly owned subsidiaries of IHI and are affiliates of ILLC. The Instinet BD Affiliates may, on behalf of their clients, send orders for execution in U.S. markets to ILLC's trading desks, SOR, and algorithmic trading strategies, many of which include the ATS as a destination.

d. If yes to Item 6(c), are the services that the NMS Stock ATS offers and provides to the entity required to be identified in Item 6(c) the same for all Subscribers?

Yes ☐ No ☐ *If no, identify and explain any differences.*

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: ILLC's system comprises an integrated Core Messaging System with numerous applications providing, reading, and consuming data messages from the Core Messaging System. The ATS system (e.g., matching engine and associated applications) and ILLC's systems used to support

its agency broker-dealer business run on the Core Messaging System. 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 Messaging System is the conduit through which all firm-wide order information is processed (e.g., ATS and agency broker-dealer order and execution information). All orders routed to the ATS pass through the Core Messaging System. This information is processed by data messages which are readable only by the applications on the Core Messaging System that have been designed and permissioned by ILLC to do so.

Each application subscribes to different message types and is permissioned to subscribe only to the message types necessary for its designated function. For example, the Instinet Trading Products (Experts, SOR, and OMS/EMS) are subscribed to utilize messages regarding the orders routed by the relevant product, including where orders were routed and/or executed, which may include the ATS or any other market center. The Instinet Trading Products may not access data messages related to other ILLC functions, including data messages related to the ATS generally, Direct Subscriber orders, ATS order priority, or counterparty information.

The BlockCross ATS consists of standalone hardware comprising dedicated servers (collectively the "BlockCross System") and software applications separate from the ILLC systems described above.

The connection between the Core Messaging System and the BlockCross System is limited. Instinet Trading Products, housed on the Core Messaging System may access the BlockCross ATS and, by extension, the BlockCross System through FIX connections, similar to any external market center. Additionally, BlockCross order and execution information are periodically copied onto the Core Messaging System, as further discussed below.

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.

BLOCKCROSS SYSTEMS WITH ACCESS TO DIRECT SUBSCRIBER CONFIDENTIAL TRADING INFORMATION: SUPPORT TOOLS: ILLC maintains support tools (i.e., applications) specific to BlockCross (the "Support Tools") designed to allow permissioned employees the ability to view certain types of data necessary to the performance of the employee's job function. Permissioned employees with access to the Support Tools may only access BlockCross data and cannot use the Support Tools to access data from other Instinet ATSs. As discussed below, ILLC grants employees access to the Support Tools necessary to perform their responsibilities and in line with ILLC's Regulation ATS WSPs.

ILLC may permission employees with full access to the Support Tools. Full access allows a permissioned employee to view and manage all data on the BlockCross System, including open orders in the ATS.

Permissioned employees will also have the ability to cancel orders in BlockCross. Permissioned employees may also view each order's status (e.g. whether the order has been matched, exposed via the Subscriber IOI functionality, or has been routed out of the ATS via an Experts strategy). Permissioned employees may also edit standing instructions on how the BlockCross System should handle each order that a Subscriber submits. Full access to the Support Tools is limited to personnel supporting the operations of the BlockCross System and compliance supervisory personnel. Employees responsible for operating the BlockCross System include Operations and Technology Personnel.

ILLC may also permission employees with read-only access to the Support Tools. Such employees can view all data described in the preceding paragraph, but they may not cancel orders or make any changes to standing instructions. Read-only access to the Support Tools is limited to Operations, Compliance, Technology, and ETP Personnel.

DESKTOP APPLICATION: The Desktop Application can transmit Subscribers' confidential trading information to the extent orders or trading interest is entered into the Front End or receives executions in BlockCross. Users with access to the Desktop Application may only access BlockCross data and cannot use the Desktop Application to access data from other Instinet ATSs.

ILLC may permission employees may with live access to the Desktop Application on a client-by-client basis. Such permissioned employees may view client orders, including open orders in the ATS specific to a given client. Permissioned employees may also view each order's status (e.g. whether the order has been matched, exposed via the Subscriber IOI functionality, or has been routed out of the ATS via an Experts strategy). Technology and ETP Personnel responsible for customer support as well as Operations and compliance personnel may be permissioned, on a client-by-client basis, to access Subscribers' confidential trading information in this manner. Such personnel provide clients technology and order routing and execution support and, accordingly, are responsible for addressing Subscriber inquiries related to orders or trading interest that has been submitted to the Front End or has been executed in BlockCross. Sales and Trading Personnel may also be permissioned, on a client-by-client basis, to access the Desktop Application to provide order and execution support and analytics to clients who request it.

ILLC may permission employees may to access the Desktop Application on a post-execution basis, which allows a permissioned employee to view orders that have been executed in BlockCross, including the identity of the parties to each trade. Access to the post-execution view is limited to Technology and ETP Personnel responsible for customer support as well as Operations and compliance personnel. Sales and Trading Personnel may also be permissioned to access the Executions Support Tool to provide post-execution support and analytics to clients who request it.

PHYSICAL ACCESS: The data on the BlockCross System is accessible through direct access to the BlockCross System servers and databases. ILLC limits physical access to the BlockCross System servers and data bases to employees responsible for operating the system and further limits access to employees performing necessary IT functions. The BlockCross System servers and databases are housed in locked rooms requiring keycard access. Entry and exit is monitored via video surveillance.

CONNECTION TO ILLC SYSTEMS: Drop copies of BlockCross orders and executions are sent to the Core Messaging System at the end of each day in a single large batch file delivered after the close of trading. Each copy contains all relevant trade data for each order. BlockCross order information that has been drop copied to the Core Messaging System. However, the BlockCross System uses a dedicated FIX connection to transmit BlockCross execution information to the Core Messaging System, in real time, for the purposes of the clearance and settlement of transactions occurring in BlockCross.

ILLC 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"). BlockCross orders and executions that have been copied to the Core Messaging System will also be written to the Core Database. This information includes both Direct and Indirect Subscriber order and execution information, 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 full Core Database via the Core Web GUI is limited to personnel supporting the operations of the Core Messaging System and related databases and compliance supervisory personnel. Employees responsible for operating the Core Messaging System 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.

ILLC limits physical access to its servers and databases to employees responsible for operating the system and generally further limits access 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.

As stated in response to Part II, Item 6, AWS provides cloud storage and retention of certain ILLC data. This information includes Direct and Indirect Subscriber order and execution information from the ILLC Core Messaging System, as well as other ILLC data. Initially, such information will be periodically transmitted to AWS for storage and retention in tandem with ILLC's internal Core Database. The purpose of this tandem transmission is to explore the feasibility of a third-party solution and replace the Core Database hardware and inhouse support tools described herein.

During this initial period, access to the Core Database will remain as described in this Part II, Item 7. Access to ILLC's data through AWS will be limited to Technology and Operations Personnel for the purpose of testing and implementing ILLC's transition to a third party solution for data storage and retention.

ILLC 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 Electronic Sales Trading component group of the ILLC trading desk are considered client coverage for all clients utilizing the Experts algorithms.

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 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 Operations Principal. In reviewing such requests, the ATS Operations Principal 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 Operations Principal'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 Operations Principal will adjust the employee's access to appropriately reflect the employee's new role. Based on this review, the ATS Operations Principal 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 Operations Principal 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 by the ATS Supervisor 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.