

## 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. As part of operating the ATS, Dealerweb has developed extensive policies, standards, and procedures to ensure that the data, information, and the related systems are protected from threats such as errors, internal and external security attacks, theft, fraud, privacy violations, embezzlement, sabotage, and natural or manmade disasters. These policies, procedures, and controls are designed to safeguard the confidentiality, integrity, and availability of the ATS platform by preventing unauthorized access to or use of a subscriber's confidential data. The primary policies and procedures currently in place to address confidentiality safeguards include: Tradeweb Information Security Policy, Tradeweb Cybersecurity Policy, Tradeweb Markets LLC Privacy Policy, Tradeweb Access Control Policy, and Dealerweb's Written Supervisory Policies and Procedures. These procedures are reviewed, tested, and updated annually at a minimum and on an ad-hoc basis when necessary and are available to all employees through the Firm's internal website. In terms of confidentiality safeguards, upon joining Dealerweb, all employees are required to sign the Fair Competition and Arbitration Agreement, acknowledging that they shall be in possession of confidential, client information and shall not disclose any confidential information without the prior written consent of the Firm. The only such instances where confidential information may be shared after receiving Firm approval would involve regulatory inquiries and / or audits initiated by regulatory agencies such as the SEC, FINRA, NFA, and MSRB and any potential legal actions which may involve disclosing client data. When an individual is no longer an employee of the Firm, as part of the termination process, the individual is required to sign an attestation that he / she will continue to treat all company information as confidential. In addition, as part of the hiring process, all employees are required to review a copy of the Firm's Written Supervisory Procedures and annually thereafter as part of the annual certification process. All employees are required to complete various internal training courses, such as the bi-annual Information Security and Privacy Awareness Training course, which confirms each employee understands their responsibilities to protect confidential information and a bi-annual Cybersecurity training course. The Firm through the Tradeweb Enterprise Risk Management Group operates continuous organization wide security programs and training courses, including regular testing related to phishing and social engineering. ~~There is no third-party vendor that has access to the Firm's ATS Platform, including the order and trading history involving EFP's and NAVX.~~ The Firm prohibits the sharing of any subscriber confidential information with anyone not authorized to receive such information and any violation of the Firm's policies and procedures concerning the safeguarding of confidential information by any employee will be met with disciplinary action, up to and including termination from the Firm. The basis of authorization for access to the ATS platform is based solely on the applicable job

functions related to the daily maintenance, monitoring and supervision of the ATS Platform and the trading activities that take place on the platform to ensure compliance with all applicable rules. The Firm has indicated in Part II, 6(a) the list of individuals and / or departments that are authorized to have access to Subscriber information based on their specific job functions, which are utilized to support the ATS Platform.

In addition to implementing various confidentiality safeguards, the Firm has also implemented various safeguards related to employee access of the ATS platform, specifically restricting which employees have access to the platform and the systems that support it based on their specific job responsibilities / functions. Please refer to Part II, Item 6a, which identifies and describes the only departments within Dealerweb and Tradeweb that have access to the ATS platform based on their specific job functions. These groups require access to support and monitor the trading activity on the platform. Prior to receiving access to the ATS Platform, an employee must first receive approval from his / her supervisor and once that approval has been granted, final approval must be granted by the Firm's Compliance Department. After obtaining all necessary approvals, an employee is provided access to the ATS Platform and will receive a unique username and password in order to login. Passwords are required to be changed every 90 days. Access is securely contained by the Firm and reviewed by the Firm. Tradeweb's Enterprise Risk Management Group conducts bi-annual reviews of all employees who have access to the Dealerweb Platform. As part of the review process, the Risk Group will send each Supervisor a list of employees that presently have access to the platform and their respective entitlements and request that each Supervisor review the access and entitlements and make any necessary changes / revisions. Each Supervisor will then communicate their changes and approval to the Risk Management Group. Upon receiving approvals from all Supervisors, the Risk Management Group will make all necessary entitlement changes and then send the list to Compliance for review and approval. The Firm's Compliance Department (CCO and / or designee) will review the list and communicates its approval of entitlement access to the Risk Management Group. These reviews and approvals between the Risk Management Group, Supervisors, and Compliance are conducted via email. As indicated further in 7d, approved access to the platform provides an employee with access to all orders and executed transactions for each subscriber for both EFPs and NAVX.

In regards to employee trading, the Firm allows employees to maintain outside brokerage accounts with third party brokers. As required under FINRA Rule 3050, employees are required to disclose all outside brokerage accounts under their control to the Firm and provide the Firm with access to all trading confirmations and account statements. In terms of trading restrictions, the Firm's Securities Trading Policy does not allow its employees and immediate family members to participate in any IPO's and sell short or engage in speculative transactions involving Tradeweb Markets Inc.'s common stock, TW, which is listed on the Nasdaq National Market. At the end of each month, the Firm's Compliance Department conducts a review of all employee statements for the following activity: any transactions executed in an IPO, any short sales and / or speculative trading in TW common stock, trading activity suggestive of the use of confidential information, and any additional, excessive trading activity, such as frequent day trading. The Firm prepares a written analysis each month detailing its reviews of employee trading, which is distributed to all members of the compliance department. Please note that Dealerweb does not conduct any proprietary trading, investment banking activities, and / or offer any fundamental equity or fixed

**income research as defined in FINRA Rules 2241 and 2242. In addition, the Firm is not a party to any of the EFP or NAVX transactions as the Firm gives up all transactions for execution to each subscriber.**

-As disclosed above in Part II, Item 6.a, Dealerweb, through a licensing arrangement with its parent company, Tradeweb Markets Inc., utilizes Nasdaq SMARTS Trade Surveillance system for trade surveillance purposes. Real time order and trade data, including live bids and offers entered by subscribers into the Dealerweb Platform for EFP and NAVX feed into Nasdaq SMARTS. There are specific alerts generated through Nasdaq SMARTS based on parameters established and reviewed by Dealerweb Regulatory Compliance. In order to review these alerts, members of Regulatory Compliance log into Nasdaq SMARTS with a unique username and password. Tradeweb Markets Inc. has entered into a specific agreement with Nasdaq Market Inc. to utilize its Nasdaq SMARTS Trade Surveillance System and under this agreement, all real time order and trading activity received by Nasdaq SMARTS from Dealerweb is treated as confidential and subject to Nasdaq's internal safeguards and Information Security Policy and Procedures. as well. Tradeweb's Enterprise Risk Management Team conducts an annual vendor review of Nasdaq SMARTS, which includes reviewing and evaluating Nasdaq's Information Security Policy and other internal safeguards.

b. 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)? **No**

c. 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 the applicable rules)? **No, not applicable.**

d. 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. **Please refer to Part II, Item 6a of this form for additional information. The enclosed list contains the list of departments and / or business units within Dealerweb and / or Tradeweb that have access to some or all of the confidential order and trade data for subscribers that trade on the EFP and NAVX Platforms. The basis for approved access for these departments and / or business units is to service and / or support the Dealerweb ATS platform. As discussed in Item 7a above, employee access to the ATS Platform must first be approved by the employee's supervisor with final approval obtained from the Firm's Compliance Department. The list of departments and business units granted access to perform the necessary job functions in order to support the ATS platform are as follows:**

- Dealerweb Market Support – this group is responsible for monitoring the platform to resolve subscriber issues and is the primary team monitoring the market for potential technology issues.
- Dealerweb Product Management – this group is responsible for providing relationship management support for subscribers across all of the Firm’s products, which trade on the Firm’s ATS and NMS Stock ATS.
- Dealerweb EFP Trade Support - Liaison with subscriber trading desks to address potential trade related issues, obtaining trade affirmation, where necessary, and reporting the futures leg of EFPs to the applicable futures exchange.
- Dealerweb Tech Operations & QA – this group is responsible for all technical issues with the platform including the testing of any changes.
- DW Operations – this team is responsible for TRF and CATOATS reporting.
- Tradeweb Enterprise Risk Management – conducts general risk management throughout the firm including providing support on the development of policies and procedures and coordinating the testing of those policies and procedure.
- Dealerweb Compliance – this team is responsible for providing guidance on applicable statutes and regulations to the business, interacts with various regulators to address inquiries, audits, and other matters, and monitors for regulatory compliance.
- Dealerweb Finance – this group is responsible for billing clients and financial reporting.
- Dealerweb & Tradeweb Senior Management – the President of Dealerweb and Chief Administration Officer of Tradeweb have view only access, which allows them to manage and supervise the business.

All business units and / or departments described above, with the exception of the Dealerweb Market Support Group have view only access to real time and historical order and trading activity for both the EFP and NAVX through the Master Blotter within Dealerweb Viewer including and all live bids and offers that have been entered by all subscribers. As a result of this access, the aforementioned business units are able to see all orders and executed transactions for both EFPs and NAVX, including all order and trade details, such as the security, quantity, price, counterparty, and name of the trader from each subscriber who entered the order and / or executed the transaction. Please note Dealerweb Market Support has the ability to cancel orders on behalf of subscribers based on written instructions received from subscribers.

As disclosed in Part II, Items 6.b and Items 7.a., Dealerweb utilizes Nasdaq SMART’s trade surveillance system. Real time order and trade information is shared by Dealerweb with Nasdaq SMARTS and alerts are generated based on parameters established by Dealerweb’s Regulatory Compliance Team. Members of Dealerweb’s Regulatory Compliance and Tech Ops teams have access to Nasdaq SMARTS through a web-based application with a unique username and password. Access to Nasdaq SMARTS requires approval from the employee’s manager and final approval from Dealerweb’s Chief Compliance Officer.