

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 StockATS, 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.

DATA PROTECTION:

Client data protection (including the protection of subscriber confidential trading information) is governed by formally instituted policies. Records containing clients' data stored in IBKR's databases, as well as on tape backups, are encrypted. Encryption algorithms, ciphers, and key parameters are consistent with the industry best practices. In addition to technical data protection measures, IBKR administers mandatory security awareness training to all its employees emphasizing data protection best practices.

INFORMATION BARRIERS:

Interactive Brokers Group ("IBG") has in place barriers designed to help ensure that confidential information relating to subscriber orders in the ATS is maintained on systems that are separate from, and inaccessible by, IBKR's affiliates (except as set forth in Part II, Item 6.b). IBKR compliance personnel review various daily, monthly and quarterly reports intended to help identify potential instances of IBKR customer information (including ATS confidential trading information which, for the avoidance of doubt, includes confidential trading information of Liquidity Providers) being impermissibly accessed by employees of IBKR affiliates. IBKR compliance personnel also review a sample of communications between IBKR personnel and personnel of its affiliates to assess whether subscriber confidential trading information is being impermissibly accessed or shared.

All new IBKR employees must review the IBG Information Barrier Policy, which is included in the IBG employee manual, and must acknowledge receipt of the current version of the IBG Information Barrier Policy annually. The IBG Information Barrier Policy states that employees of IBG and its affiliates (including IBKR employees) shall treat customer trading information (including subscriber trading information) as confidential and shall only share such information to the extent reasonably necessary to provide the relevant services and otherwise service the relevant account. As applied to ATS confidential trading information, the IBG Information Barrier Policy limits the sharing of such information within IBG to the extent reasonably necessary for the operation of the ATS and related systems (that is, IBKR's market data, clearing, stock borrow and audit trail systems), and to ensure the ATS' compliance with applicable law. In addition, IBG provides training regarding the confidentiality of customer orders and information.

ACCESS TO SUBSCRIBER CONFIDENTIAL TRADING INFORMATION:

Access to IBKR trading systems, including those that maintain ATS confidential trading information, is limited to authorized individuals. Prior to granting any employee, shared employee, or third-party service provider access (each an “**Accessing Party**”) to ATS data, IBKR reviews the level of access requested, the roles and responsibilities of the prospective Accessing Party, and the proposed uses of the data to which the prospective Accessing Party would have access. As a threshold matter, access to ATS confidential trading information is limited to individuals responsible for either the operation of the ATS and related systems (that is, IBKR’s market data, clearing, stock borrow and audit trail systems), or the ATS’ compliance with applicable law. As noted above, the IBG Information Barrier Policy provides that Accessing Parties may only use ATS confidential trading information to the extent necessary to fulfill their responsibilities regarding the operation of the ATS and related systems (that is, IBKR’s market data, clearing, stock borrow and audit trail systems), or the ATS’ compliance with applicable law; Accessing Parties are expressly prohibited from sharing ATS confidential trading information with Brokerage Customers and other clients of IBKR (e.g., Liquidity Providers and introducing brokers), except where such confidential trading information belongs to the relevant Brokerage Customer or client (e.g., information regarding a Brokerage Customer’s own orders or transactions). Individuals responsible for liquidity provision and/or trading activities on behalf of Affiliated Liquidity Providers are not permitted to access confidential trading information of the ATS.

For clarity, information regarding a subscriber’s own orders and executions within the ATS is displayed to such ATS subscriber, although IBKR treats the identity of the subscriber who submitted an order or was party to a transaction as subscriber confidential information.

Further, certain subscriber order information is disseminated, on a non-attributed basis, to GFIS for further dissemination and display to ATS subscribers. For clarity, GFIS’ role in disseminating market data to ATS subscribers is mechanical. GFIS receives non-attributed data that has already been processed by IBKR for further distribution to ATS subscribers. GFIS does not receive or otherwise have access to “attributed” ATS order and execution data (that is, GFIS does not have access to order or execution data identifying the subscriber that submitted the order or was party to a trade) or to any other ATS data that is not shared with ATS subscribers. GFIS does not have any employees.

Access to internal systems and applications is provisioned on the least-privilege basis and controlled using passwords or, in some instance, multi-factor authentication (MFA). In particular, MFA is used for all remote access and also for onsite access to particularly sensitive systems. Password length and complexity requirements are established and enforced.

Periodically, as prescribed by IBKR’s policies and procedures, all employees, shared employees, and third party service providers are reviewed to determine whether their level of access to ATS data is appropriate. This includes assessing whether the Accessing Party continues to have responsibilities in connection with

the operation of the ATS or the ATS' compliance with applicable rules.

Access to IBKR office and data center spaces is strictly controlled and limited to authorized personnel. Electronic door entry systems are in use and configured to allow personnel access only to the areas required to fulfill their job functions. Additionally, video recording/surveillance systems are employed in data centers and select office locations. Activity logs, including records of permitted and denied entry attempts captured by the access control and footage of the video surveillance system, are maintained.

EMPLOYEE TRADING:

The IBKR Employee Trading Policy prohibits IBKR employees from trading securities or commodity futures between the hours of 8:30 a.m. and 6:00 p.m. in their time zone.

All IBKR employees, at onboarding and annually thereafter, are reminded of their obligation to identify all brokerage accounts in which the employee or any related person (as noted at FINRA rule 3210/.02) maintains an interest, including any brokerage accounts subsequently opened. IBKR obtains copies of such employee's account statements and trade confirmations from the relevant brokerage firm. IBKR prohibits an employee from opening or otherwise maintaining an account with a brokerage firm that will not provide IBKR with duplicate account statements and trade confirmations. IBKR compliance and supervisory personnel review employee account statements and trade confirmations on a monthly basis. As part of these reviews, IBKR compliance and supervisory personnel assess whether an employee has violated IBKR's Employee Trading Policy, including any indication of misuse of subscriber confidential trading information (in particular, the IBKR Employee Trading Policy, among other things, prohibits employees from trading on the basis of material non-public information). Employee trading conduct specifically reviewed for includes particularly active accounts and trading in any restricted securities outside of the "open window" period (presently limited to securities issued by Interactive Brokers Group, Inc.).

- 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)?*

Yes No

If yes, explain how and under what conditions.

- 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 applicable rules)?*

Yes No

If yes, explain how and under what conditions.

- 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.*

Programming and technology personnel involved in operating IBKR's systems, including operation of IBKR's order management systems, SOR, matching engines and order gateways have live audit trail access and, as such, may be able to view, on a non-anonymized basis, an order that has been routed to the ATS (including, for clarity, non-anonymized information regarding both Displayed Orders and Non-Displayed Orders). System administration and IB risk departments also have live audit trail access, including non-anonymized order and execution information (including, for clarity, non-anonymized information regarding both Displayed Orders and Non-Displayed Orders).

Personnel responsible for IBKR's clearing operations, stock borrow operations, audit trail reporting and the generation of account statements, as well as members of IBKR's compliance department, have access to post-trade information which may include information relating to transactions effected in the ATS.

Part III: Manner of Operations

Item 21: Trade Reporting

- a. *Explain any procedures and material arrangements for reporting transactions on the NMS Stock ATS, including where an ATS reports transactions and under what circumstances.*

The ATS maintains daily summaries of trading and time-sequenced records of order information, including the date and time the order was received, the date, time, and price at which the order was executed, and the identity of the parties to the transaction. As the ATS only effects transactions outside regular trading hours, trades executed in the ATS are reported by ~~8:15 AM~~4:15 AM ET following the end of the relevant trading session (that is, for a trading session that operates from 8:00 PM ET Monday through 3:50 AM ET Tuesday, trades effected during that trading session are reported by ~~8:15 AM~~4:15 AM ET Tuesday).

IBKR reports all trades in the ATS to either the NASDAQ TRF Carteret and the NASDAQ TRF Chicago in either case using the IEOS MPID. IBKR's systems utilize load-balancing programming (e.g., network traffic optimization) in determining whether to report a particular transaction to the Chicago or Carteret NASDAQ TRF.

- b. *Are the procedures and material arrangements for reporting transactions on the NMS Stock ATS the same for all Subscribers and the Broker-Dealer Operator?*

Yes *No*

If no, identify and explain any differences.