* * * * *

**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.**

The BIDS ATS is a wholly-owned subsidiary of Cboe Global Markets, Inc. ("Cboe"), which operates national securities exchanges in the U.S. BIDS ATS personnel and Cboe personnel are subject to policies and procedures that are designed to preserve the independent governance and operation of the U.S. equities business of the BIDS ATS ("Cboe Policies and Procedures"). The Cboe Policies and Procedures include information barriers between the equities businesses of the BIDS ATS and Cboe's U.S. national securities exchanges. The information barriers prohibit access to or receipt of any nonpublic information concerning the BIDS ATS equities business, including Confidential Data (as defined below), by any Cboe personnel that provide services to or on behalf of Cboe's U.S. national securities exchanges ("Cboe Exchanges"). The ATS Oversight Committee, an independent committee of the Cboe Board of Directors, is responsible for overseeing those businesses of BIDS, such as the U.S. equities business, that involve assets also traded on a U.S. national securities exchange subsidiary of Cboe. One of the responsibilities of the ATS Oversight Committee is to oversee, review, approve and make determinations with respect to the adequacy and effectiveness of the information barriers in the Cboe Policies and Procedures.

Cboe monitors and enforces the information barriers through a series of controls and surveillance processes and further supports them through both technological separations and physical separations. For example, BIDS personnel are required to work in a separate office building, or in a separate workspace in the same office building, from Cboe personnel with controls that are sufficient to prevent BIDS personnel from accessing areas designated for the exclusive use of Cboe personnel, and vice versa (e.g., via requiring badge access, locating the workspaces on separate floors, walls and locked doors), subject to limited exceptions (e.g., for personnel who perform corporate support functions). In addition, the Cboe Policies and Procedures require that the BIDS ATS operate on separate technology and servers from the Cboe Exchanges, and that the data center space housing the BIDS ATS servers must be separate from that housing the servers of the Cboe Exchanges (e.g., separate cages).

The Cboe Policies and Procedures expressly state that, in addition to the information barriers certain information concerning BIDS (in particular, client information) is subject to confidentiality obligations set forth in BIDS's client contracts, BIDS's Form ATS-N and/or

other legal or regulatory requirements (collectively, "Other Confidentiality Obligations"). Pursuant to the Cboe Policies and Procedures, the information barriers are in addition to the Other BIDS Confidentiality Obligations, and nothing in the Cboe Policies and Procedures creates any exception to, or otherwise limits, the Other BIDS Confidentiality Obligations. The BIDS ATS operates as a dark venue and does not disclose confidential information to third parties, other than as needed to complete transactions or comply with securities laws and regulations as discussed in this Part II, Item 7 or elsewhere in this Form ATS-N.

Confidential Data is defined as:

**Gateway Logs:** Transaction logs for protocol gateways connecting from order management systems ("OMS")/execution management systems ("EMS") to the BIDS ATS

**Firm Order Information:** Information regarding all Firm orders.

**Conditional Information**: Information regarding Conditionals and invitations in the BIDS ATS.

**AIOI Information**: Information regarding all AIOIs in the BIDS ATS.

**Trade Information:** Trades in the BIDS ATS during the live trading session.

**Sponsor Settings:** Administrative settings and risk limits of Sponsored Firms managed by Sponsors.

**Scorecards and Filter Settings:** BIDS Scorecard values for Traders and Filter settings set by Traders (discussed in Part III, Items 7 and 9).

**Trader Configuration:** Preferences set by Traders for Firm order and Conditional interaction on the BIDS ATS.

**Database Information:** Transaction and configuration data stored in the BIDS ATS databases.

**Server Logs:** Log files generated by the BIDS ATS applications.

Given the sponsored access model made available by BIDS (discussed in Part III, Item 2), BIDS provides each Sponsor with information related to any Firm order, Conditional, or trade on which that Sponsor has been designated by a Sponsored Firm. BIDS does not engage in any trading activities other than activity in connection with the operation of the BIDS ATS as described in this Form ATS-N and, as a result, does not engage in activities that may be deemed in conflict with the BIDS ATS.

As part of operating the BIDS ATS, BIDS maintains written policies, procedures and controls ("Confidentiality Safeguards") designed to safeguard the confidentiality, integrity and availability of the BIDS ATS by preventing unauthorized access to or use of Participants' Confidential Data. The Confidentiality Safeguards include:

a. Guidance with Respect to Handling Information: Confidentiality and Privacy Policy
b. Cybersecurity Policy
c. Compliance Manual
d. Supervisory Procedures

The Confidentiality Safeguards are reviewed, tested and updated regularly as described below. Key aspects of the Employee Access Safeguards and the System Safeguards prescribed by the Confidentiality Safeguards are summarized below.

As part of the Confidentiality Safeguards, BIDS requires that all employees and independent contractors of BIDS and BTT, (collectively referred to as "employees") acknowledge receipt and review of applicable BIDS' written policies at the time of hiring, and at least annually thereafter. In addition, all employees must complete security awareness training as part of the onboarding process and complete periodic confidentiality training during employment. BIDS also operates a continuous, organization-wide security awareness program that includes regular testing related to phishing and social engineering.

## EMPLOYEE ACCESS SAFEGUARDS

### A. Employee Access Safeguards

BIDS strictly limits the employees that may access the live BIDS ATS production networks, databases, servers, and ATS applications (collectively, the "BIDS Systems") and data to those employees that must have such access to perform their jobs. BIDS enforces these protections by implementing access controls around the BIDS Systems. Permitted employees can only access these BIDS Systems through a secure authentication process.

1. Access Controls:

a. Access to BIDS Systems and data is restricted to authorized employees based on job responsibility and approved in advance by management. BIDS management regularly reviews access rights to BIDS Systems.

b. Data in the BIDS ATS is partitioned by Participant and Trader. BIDS management regularly reviews and tests access control rules in the BIDS ATS.

2. Authentication:

a. Individual employee access must be authenticated and is reviewed by BIDS management.

b. Credentials for and access by administrative users are securely maintained and reviewed regularly by BIDS management.

c. BIDS network services (e.g., BIDS ATS, BIDS Windows Active Directory) automatically enforce password complexity and password aging rules for access.

d. BIDS requires multi-factor authentication for remote access by employees through secure VPN tunnels.

3. Logging:

a. Firm orders, Conditionals, trades and application configuration changes in the BIDS Systems are time-stamped and recorded in logs.

b. Clocks on BIDS Systems devices are synchronized using Precision Time Protocol ("PTP") to ensure that timestamps are accurate and consistent. PTP is an industry standard protocol used to synchronize computer clocks with a high degree of accuracy.

c. Ad hoc queries and ad hoc changes made to the BIDS ATS database are logged and reviewed on a regular basis by BIDS management.

**B. Trading by Employees**

Other than operating the BIDS ATS as described in this Form ATS-N, BIDS does not engage in trading and, as a result, does not have employees responsible for trading activities. BIDS does, however, permit employees to maintain personal investment accounts with third party brokers. Employees are required to disclose to BIDS all personal trading accounts controlled by the employee (and other related accounts as set forth in BIDS' policies[1], collectively "outside accounts") and provide BIDS with access to trading confirmations and account statements for these outside accounts. With access to this information, the firm's compliance department reviews and monitors trading by all employees. Employees must request and receive prior compliance approval for all transactions in covered securities (i.e., securities eligible to be traded on the BIDS ATS) for themselves or in their outside accounts.

As part of the employee trading review, the compliance department compares the requested transactions to activity on the BIDS ATS at the time of the request to verify that recent transactions on the BIDS ATS and confidential information available to the BIDS ATS does not appear in conflict with the employee trade request. Any appearance of potential conflict would cause denial of the trade request and an investigation of whether any conflict exists. In addition to prior approval, employees must hold positions in covered securities for a minimum of 30 days, with certain limited exceptions.

**SYSTEM SAFEGUARDS**

**In addition to internal controls, BIDS has established rigorous safeguards designed to protect the BIDS Systems and the Confidential Data processed by the systems from external threats, as set forth below.**

**A. Physical Security**

[1] Employee accounts also include accounts of the employee's spouse, partner, minor children and other members of the employee's household and any account in which the employee has an interest or has the power, directly or indirectly, to make or influence investment decisions (any person who is supported, directly or indirectly, to a material extent by the employee).

The BIDS Systems are hosted in Equinix data centers and subject to high security standards, including video surveillance, 24x7 armed security, and multi-factor physical access. The physical and operational security controls at these data centers are assessed by independent third parties annually. The facilities maintain multiple backup power systems to help ensure continuous operation in the event of electrical power failure.

### B. Network Security

Participants access the BIDS ATS through point-to-point network cross connects, managed private networks, or over secure Internet connections. Data in transit over the Internet is encrypted. In addition, BIDS employs firewalls to isolate the BIDS Systems from the Internet.

### C. Network Monitoring

BIDS forwards BIDS Systems, network, and application logs to a secure, write-once log aggregation system for analysis and alerting for BIDS engineering, IT and operations staff. BIDS monitors and protects its networks using a security intrusion detection system (IDS) and intrusion prevention system (IPS) on a 24x7x365 basis.

### D. Web Access and Email

BIDS has in place an enterprise Data Loss/Threat Prevention (DLP/DTP) solution and web proxies to monitor and filter outbound email and web traffic from inside BIDS networks. BIDS uses an email gateway service to filter all inbound email. Participants can request encrypted emails through bi-directional enforced transport layer security (TLS) connections.

### E. Vulnerability Management

BIDS scans all BIDS networks on a regular basis for vulnerabilities. The results of scanning are reviewed by BIDS engineering, IT and BIDS management. If issues are identified, remediation activities are scheduled and undertaken. Firewall patches are applied on a regular basis, based on vulnerability severity and operational risk considerations.

### F. Risk Management

BIDS maintains an organization-wide operational risk management program that includes ongoing assessments of strategic, environmental, financial, compliance, security and operational risks. This risk management program is subject to ongoing review and update by BIDS management, including a review of any operational and security incidents, vulnerability management programs, penetration tests and other assessments, and the status of control programs.

### G. Third-Party Supplier Management

BIDS performs risk-based reviews (by legal, compliance and management) of third-party supplier relationships at the time of engagement and on an annual basis. The initial review includes consideration of the service levels to be performed, potential strategic risk, and the security and confidentiality controls of the supplier. In addition, BIDS may require a non-disclosure agreement or similar provisions as part of a third-party supplier relationship.
On an annual basis, BIDS operations and compliance reviews third-party suppliers. As part of this annual review, BIDS operations and compliance identify critical suppliers and review their security and confidentiality controls. The results of this annual review are recorded and approved by BIDS management.

**H. Incident Response**

BIDS maintains a cyber security incident response program which involves BIDS ATS operations, engineering, IT, compliance and legal staff, and BIDS management. A Computer Security Incident Response Plan ("CSIRP") lays out clear procedures and responsibilities for handling of security incidents including the loss or theft of Confidential Data, and violations of security protocols. BIDS management reviews and tests the CSIRP at least annually.

**I. Security Assessments and Audits**

Existing security controls (including those described in this Part II, Item 7) are reviewed and tested by BIDS management on a regular basis, including scheduled vulnerability scanning and penetration testing, operational and security checks, quarterly and annual BIDS management reviews, and ad hoc checks. The results of these reviews are retained for internal control and audit purposes.
In addition to BIDS management and BIDS compliance reviews, BIDS contracts with third party providers to conduct security tests, audits, and assessments, including the following:

1. Network penetration/vulnerability testing (at least annually)
2. Application penetration testing (at least annually)
3. Annual IT control audit
4. Annual SOC 2 Type II assessment of BIDS ATS security and confidentiality controls

The results of these tests, audits, and assessments are reviewed with BIDS management.

**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 X**

**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.**

The list below sets forth a summary of roles and responsibilities of the employees who have access to some or all Confidential Data. With regard to each employee role, the basis for approved access to the Confidential Data is to service or support the BIDS ATS in line with the responsibilities of the particular role.

As a general matter, BIDS restricts access to Confidential Data solely to those employees who have a need to know in order to assure the efficient and uninterrupted operation of the BIDS ATS.

**1. Role of Permissioned Employee: <u>ATS Sales Support</u>**

**a. Responsibilities**
- i. Sales support covering Participants;
- ii. Provide training to Participants' staff;
- iii. Assist Participants with use of the BIDS ATS;
- iv. Participant reporting and management reporting

**b. Confidential Data subset that ATS Sales Support can access is limited to:**
- i. Trader Configuration;
- ii. Firm order Information;
- iii. Conditional Information;
- iv. AIOI Information;
- v. Trade Information;
- vi. Sponsor Settings;
- vii. Scorecards and Filter Settings

**c. Additional Information**
- i. Licensed sales/customer service personnel;
- ii. Access approved by Head of Sales;
- iii. ATS Sales Support employees have access to the Confidential Data of Participants as required for support and sales purposes; and
- iv. Access to data through application query screens and admin screens

**2. Role of Permissioned Employee: <u>ATS Integration Desk</u>**

**a. Responsibilities**
- i. Onboarding and set-up of Participants and Traders;
- ii. Day-to-day monitoring and support of connectivity to the BIDS ATS;

iii. Resetting BIDS ATS credentials on request of Traders;
iv. First level application support – troubleshoot common connectivity and operational issues

**b. Confidential Data subset that ATS Integration Desk can access is limited to:**

i. Trader Configuration;
ii. Firm order Information;
iii. Conditional Information;
iv. AIOI Information;
v. Trade Information;
vi. Sponsor Settings;
vii. Scorecards and Filter Settings;
viii. Gateway Logs

**c. Additional Information**

i. Licensed help desk personnel;
ii. Access approved by Chief Operating Officer (COO);
iii. Session command-line and database activities are logged and reviewed by BIDS management

**3. Role of Permissioned Employee: <u>ATS Operations</u>**

**a. Responsibilities**

i. Day-to-day ATS operational support, including job scheduling and job recovery;
ii. Application monitoring and alert management;
iii. System configuration changes, configuration reviews/health checks;
iv. Deploy changes/upgrades to ATS software;
v. Data archival and data repair;
vi. Ad hoc data analysis and queries;
vii. Second level application support – incident response, problem investigation and recovery

**b. Confidential Data that ATS Operations can access:**

i. Trader Configuration;
ii. Gateway Logs;
iii. Firm order Information;
iv. Conditional Information;
v. AIOI Information;
vi. Trade Information;
vii. Scorecards and Filter Settings;
viii. Sponsor Settings;
ix. Database Information;
x. Server Logs

**c. Additional Information**

i. Engineering personnel;
ii. Access approved by COO;
iii. Session command-line and database activities are logged and reviewed by BIDS management

**4. Role of Permissioned Employee: <u>BIDS Compliance</u>**

**a. Responsibilities**
i. Regulatory compliance for BIDS and the BIDS ATS

**b. Confidential Data subset that BIDS Compliance can access is limited to:**
i. Trader Configuration;
ii. Firm order Information;
iii. Conditional Information;
iv. AIOI Information;
v. Trade Information;
vi. Sponsor Settings;
vii. Scorecards and Filter Settings

**c. Additional Information**
i. BIDS compliance employees have access to the Confidential Data of Participants as required for compliance purposes;
ii. Access to data through application query screens and admin screens;
iii. Access approved by COO

**5. Role of Permissioned Employee: <u>Developers on Call</u>**

**a. Responsibilities**
i. Assist ATS Operations with problem investigation, diagnosis and recovery;
ii. Application monitoring and alert management;
iii. Assist with software deployment/changes as required by ATS Operations;
iv. Ad hoc data analysis and queries;
v. System performance analysis and tuning;
vi. Third level application support – problem recovery, root cause analysis, software patching

**b. Confidential Data that Developers on Call can access:**
i. Trader Configuration;
ii. Gateway Logs;
iii. Firm order Information;
iv. Conditional Information;
v. AIOI Information;
vi. Trade Information;
vii. Scorecards and Filter Settings;

viii. Sponsor Settings;
ix. Database Information;
x. Server Logs

**c. Additional Information**

i. Senior developers on support rotation, accessing BIDS ATS system/data as requested by ATS Operations or the ATS Integration Desk;
ii. Access approved by COO;
iii. Session command-line and database activities are logged and reviewed by BIDS management

**6. Role of Permissioned Employee: <u>ATS Analytics and Reporting</u>**

**a. Responsibilities**

i. Analytics and management reporting, metrics and statistics;
ii. Ad hoc queries and analysis on request of ATS Sales Support or management

**b. Confidential Data subset that ATS Analytics and Reporting can access is limited to:**

i. Trader Configuration;
ii. Firm order Information;
iii. Conditional Information;
iv. AIOI Information;
v. Trade Information;
vi. Scorecards and Filter Settings;
vii. Sponsor Settings;
viii. Database Information

**c. Additional Information**

i. Licensed personnel and senior developers;
ii. Access approved by COO
iii. Session command-line and database activities are logged and reviewed by BIDS management

**7. Role of Permissioned Employee: <u>System Engineering</u>**

**a. Responsibilities**

i. Provision, configure, monitor and support the runtime infrastructure (servers, network, databases) for the BIDS ATS;
ii. System utilization and performance analysis and tuning;
iii. BIDS Operations user set up; Incident response, troubleshooting and recovery

**b. Confidential Data subset that System Engineering can access is limited to:**

i. Confidential Data stored on infrastructure devices that are managed by the engineer

**c. Additional Information**

i. Engineering personnel;

ii. Access approved by COO

**8. Role of Permissioned Employee: <u>IT Administrators</u>**

**a. Responsibilities**

i. Engineering and operational support of office IT applications and services

**b. Confidential Data subset that IT Administrators can access is limited to:**

i. Working copies of Confidential Data that may be held on BIDS personnel desktops or in email

**c. Additional Information**

i. IT desktop support personnel;

ii. No direct access to the BIDS ATS trading systems

* * * * *