

## **Part II, 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**

GSCO has written policies and procedures designed to safeguard confidential trading information. Such policies and procedures are global and, as such, apply to The Goldman Sachs Group, Inc. and all of its affiliates (e.g., GSCO, GSI and other affiliates). GSCO considers information about Participants' identities, orders, transactions, strategies, and activities to be confidential trading information subject to protection. GSCO and Affiliate employees' access to Participant confidential trading information is dependent upon the level of information that is needed to perform their duties and responsibilities related to Sigma X2 ("need to know standard"). GSCO and Affiliate employees are strictly prohibited from using such information in an unauthorized manner and from discussing the details of any trades executed in Sigma X2 with persons who do not need such information to carry out their designated duties and responsibilities. Access to such information is granted as needed to perform these duties and responsibilities (i.e., real-time or delayed, isolated, periodic, or continuous). The individuals and systems with access to Participant confidential trading information, including the basis for such access, are outlined in response to Part II, Item 7.d. Set forth below are the policies and procedures in place to safeguard and oversee the protection of Sigma X2 Participant confidential trading information.

### **SEPARATION OF SYSTEMS AND EMPLOYEES:**

The Sigma X2 matching engine is physically separate from other GSCO systems as it is hosted and operated by Ocean on a daily basis (i.e., Sigma X2 does not share rack space with any other GSCO systems). Similarly, the Sigma X2 matching engine and order entry servers are on separate hardware from other systems hosted/operated by Ocean. Additionally, the Ocean employees that are responsible for the daily operation of Sigma X2 and that have access to the Sigma X2 order book are in a separate physical location from GSCO employees.

GSCO employees with access to real-time Participant confidential trading information are in a different physical location on the floor, separate from GSCO principal trading employees.

### **THIRD PARTY ACCESS PROTECTIONS:**

Certain Ocean and Nasdaq employees have access to Participant confidential trading information. Such employees include Ocean and Nasdaq staff from Compliance, Operations, Technology Development (including trading and surrounding systems), Product Management, and Business Management. The confidential trading information consists of information regarding individual orders and executions, names of Participants, and volume of orders in Sigma X2.

Ocean's policies and procedures employ a three-pronged approach to permission access to Sigma X2. First, an employee must complete compliance training specific to the Ocean business unit. Second, an Ocean employee must request, and Ocean

Compliance must approve, access to each specific system based on the employee's designated role and responsibilities. Third, once approved, the Ocean employee must complete Ocean's annual Compliance training.

Ocean employees that have access to confidential trading information are subject to Ocean's "Information Barriers and Conflict Management Policies and Procedures."

All Ocean employees are subject to Nasdaq's Global Trading Policy ("GTP"), which outlines all requirements and restrictions related to personal trading activity including holding periods, annual attestations, IPO restrictions and a prohibited list. Ocean employees are required to disclose personal investment and brokerage accounts, positions, and transactions. Nasdaq's Global Ethics Team monitors personal trade activities against the GTP.

Ocean also conducts electronic communications reviews to identify policy violations including non-compliance with the above referenced policies and procedures.

GSCO has the right to audit Ocean's operation of Sigma X2, including Ocean's access to and use of Participant confidential trading information either through audits conducted by GSCO's own audit team or by third-party auditors. Such audits may be conducted on-site or off-site.

Ocean also is obligated to notify GSCO of any actual or suspected unauthorized access to confidential information, which includes Participant confidential trading information, in a timely manner.

#### GSCO ACCESS PROTECTIONS:

Access to Sigma X2 is controlled through permission configurations that provide application access only to entitled users (i.e., users who require access to information to carry out designated duties and responsibilities as described in Part II, Item 7.d. below). Access entitlements are approved by designated supervisors and documented, tracked and monitored. Designated supervisors attest periodically, via an electronic system, that procedures designed to safeguard and protect Participant confidential trading information were followed. Such procedures include reviews of organizational structure including any new or transferred employees as well as reviews of any personal account trades and any related firm/divisional policy violations (as described below).

GSCO employees with access to the Sigma X2 order book are prohibited from writing code (i.e., order handling logic) for the GSCO SOR and GSCO algorithms.

GSCO also has detailed written firm-wide and divisional policies and procedures designed to monitor and limit employee personal trading globally. As such, they are applicable to The Goldman Sachs Group, Inc. and all of its affiliates and, accordingly, are applicable to all GSCO employees, including those with duties and responsibilities related to Sigma X2. Specifically, GSCO employees are prohibited from engaging in personal trading activity that, among other things, would conflict with or appear to conflict with client business or negatively impact client service or trading outcomes. To address potential conflicts of interest GSCO employs personal trading controls including the following: (i) requiring disclosure of all covered personal trading accounts for activity monitoring purposes; (ii) requiring supervisor pre-approval before trading in single name securities; and (iii) restricting or performing enhanced reviews of personal trading in certain financial instruments. The Global Markets Division Goldman Sachs FICC and Equities, within which Sigma X2 is operated within GSCO, also has a divisional policy that provides general guidelines for limits on personal trading volumes in single name securities. The policy is applicable to all employees within Goldman Sachs FICC and Equities, including employees that have duties and responsibilities related to Sigma X2

(e.g., Supervision (including GSET managers), GSET Engineers, and GSCO and GSI Execution Coverage employees described in Part II, Item 7.d). Control-side and other employee groups described in Part II, Item 7.d (Compliance, Legal, Internal Audit, Operations) are subject to more restrictive policies regarding trading in single name securities (i.e., with limited exceptions, such employees may not transact in single name securities). GSCO supervisors must escalate personal trades if there is an appearance of impropriety (e.g., potential front-running). Additionally, GSCO employees are only allowed to use external brokerage accounts under certain terms and conditions and only with approved brokers. Finally, GSCO employee trades in certain products (e.g., single name securities) are subject to a 30-day holding period.

On an annual basis, GSCO employees (including those with duties and responsibilities related to Sigma X2) participate in compliance training that addresses information protection and client confidentiality. Additionally, on a firm-wide basis GSCO continuously monitors electronic communications to identify potential policy violations.