Privacy Policy

A) Privacy Act Disclosure

In the course of regular business activity, customers may provide personal information about themselves. Under the Gramm-Leach-Bliley Act, Introducing Brokers ("IBs") registered with the Commodity Futures Trading Commission ("CFTC") and Members of the National Futures Association ("NFA") are required to adopt written policies for handling confidential personal information and to properly distribute those written policies. Gramm-Leach-Bliley requires a financial institution to provide its customers with a notice of its privacy policies and practices, and prohibits them from disclosing nonpublic personal information about a consumer to nonaffiliated third parties unless the institution provides certain information to the consumer and the consumer has not elected to opt out of the disclosure.

The CFTC adopted privacy rules at 17 C.F.R. Part 160 (the "CFTC Privacy Rule"), which implement the requirements of the Gramm-Leach-Bliley Act and parallel the Consumer Financial Protection Bureau's Regulation P (12 C.F.R. Part 1016). The CFTC Privacy Rule requires Signal Markets, LLC ("Signal Markets" or the "Firm"), as an NFA Member and CFTC-registered IB, to adopt policies and procedures to protect various records and customer information from nonaffiliated third parties unless the customer is provided with an initial and, except as otherwise permitted, annual "privacy notice" giving the customer the option of withholding consent to the sharing of such information.

The privacy notice must set forth, among other things:

1. A general description of the Firm's policies and practices to protect customers' non-public personal information;
2. Categories of customers' non-public personal information that is collected;
3. Categories of non-public information that is disclosed;
4. If applicable, categories of affiliates or non-affiliated third parties that may receive such information; and
5. If applicable, an explanation of a customer's right to "opt out" of having his or her non-public personal information disclosed to unaffiliated third parties and how to exercise that right.

In accordance with the CFTC Privacy Rule and NFA requirements, the Firm will provide an initial privacy notice to each of its customers who are natural persons describing the Firm's privacy policy and practices, will provide that notice no less than annually thereafter for as long as the customer relationship continues, and will provide a revised notice upon a material change to the policy or notice. NFA guidance to Members reflects this obligation by directing Members to send their privacy policy to every current customer, in addition to sending it to every new customer

when the customer opens an account. In accordance with the CFTC Privacy Rule, the Firm will do the following:

1) Provide each customer the Firm's privacy notice not later than the time the customer's account with the Firm is opened, provide the notice no less than annually thereafter to each current customer, and provide a consumer who is not a customer with notice before disclosing any nonpublic personal information about that consumer to a nonaffiliated third party. If the Firm discloses, or reserves the right to disclose, nonpublic personal information to nonaffiliated third parties outside the exceptions described below, the Firm will provide customers with an "opt out" provision in the notice and give the consumer a reasonable opportunity to opt-out before disclosing their nonpublic personal information.

2) The opt-out notice will inform the consumer: (i) that the Firm does disclose or reserves the right to disclose nonpublic personal information to nonaffiliated third parties; (ii) that the consumer has the right to opt-out of that information being disclosed; and (iii) gives a reasonable means for the consumer to exercise that option.

B) <u>The Policy</u>

The Firm and its personnel will not disclose or share any nonpublic personal information relating to any of the Firm's current or former individual consumers or customers (as such terms are defined below) except as permitted by law and as set forth below:

1) upon the prior consent of the consumer or customer;
2) with the regulatory authorities and law enforcement officials who have jurisdiction over the Firm or if the Firm is required to do so by U.S. or other applicable law;
3) to protect against fraud;
4) with service providers that perform administrative or marketing services on behalf of the Firm or to the Firm's accountants, attorneys and auditors; or
5) with affiliates, provided this information does not include "creditworthiness information" which includes information on a consumer's eligibility for credit (i.e., income) and information received from consumer reporting agencies (i.e., credit history).

C) <u>Categories of Nonpublic Personal Information</u>

Consistent with the CFTC Privacy Rule, the Firm identifies below the categories of nonpublic personal information it collects and the categories of nonpublic personal information it discloses, and the categories of affiliates and nonaffiliated third parties to whom it discloses that information. These categories will be reflected in the Firm's privacy notice.

<u>Categories of Information Collected.</u> The Firm collects the following categories of nonpublic personal information about consumers and customers, as applicable:

1) Information from the consumer or customer (e.g., name, address, date of birth, Social Security number, and financial information provided on account-opening or other forms);
2) Information about the consumer's or customer's transactions with the Firm or the Firm's affiliates (e.g., account balances, positions, and trading and account history);
3) Information about the consumer's or customer's transactions with nonaffiliated third parties (e.g., information received from a futures commission merchant or clearing firm that carries the customer's account); and
4) Information from a consumer reporting agency (e.g., a credit report).

Categories of Information Disclosed and Third Parties. The Firm does not disclose, and does not reserve the right to disclose, nonpublic personal information about its consumers, customers, or former customers to affiliates or nonaffiliated third parties except: (i) to financial service providers, such as the futures commission merchant(s) or clearing firm(s) that carry the Firm's customer accounts and process the Firm's customer transactions; (ii) to the Firm's service providers, accountants, attorneys, and auditors; and (iii) as otherwise permitted or required by law, including under the exceptions in 17 C.F.R. §§ 160.13, 160.14, and 160.15 (e.g., to protect against fraud, or to respond to regulators, law enforcement, or self-regulatory organizations such as NFA). The Firm does not disclose nonpublic personal information to nonaffiliated third parties for their own marketing purposes.

Compliance with the CFTC Privacy Rule does not substitute for compliance with any state consumer law protection requirements that may be in addition to those contained within the Privacy Act. Accordingly, a designated person shall determine for each state in which individual customers reside whether there are additional state law requirements.

The designated person will maintain a checklist indicating whether the privacy notice has been initially provided to each individual customer, whether it has been provided to that customer annually thereafter, and whether it has been provided when a material change occurs. In addition, the designated person will take appropriate action to ensure the confidential consumer information is: (i) made available only to those persons directed to by the customer or as required by law; (ii) provided only to those Firm personnel who need to have access to such information; and (iii) not inadvertently disclosed to other parties.

Customer information received by the Firm from another institution can only be used for the purpose for which it was shared and cannot be re-disclosed or re-used beyond such purpose. In addition, the Firm will not disclose to third parties consumer account number information for any marketing purpose unless the third parties are marketing the Firm's own products or services.

All consumers and customers will be provided with a clear and conspicuous notice that sets forth the Firm's privacy policy and practices. Because the Firm does not disclose, and does not reserve the right to disclose, nonpublic personal information to affiliates or nonaffiliated third parties except as permitted by law under the exceptions described above, no opt-out right is triggered



under the CFTC Privacy Rule, and the Firm's notice will state this fact rather than provide opt-out procedures, consistent with the CFTC Privacy Rule's simplified notice provisions.

D) Procedures

1) Privacy Policy Notices

a) Timing of Notices. The Firm will provide notice of its privacy policy to both consumers and customers.

b) Delivery of Notices. The privacy policy notices will be sent either by mail or electronic means (provided the consumer/customer agrees to electronic delivery).

c) Revised Notices. The Firm will send out revised privacy notices should the Firm's privacy policy and practices change.

d) Record Retention. The Firm will maintain, for a minimum of three years, copies of all notices sent as well as records evidencing when and to whom notices were provided.

2) Information Sharing Arrangements. The Firm will ensure that all agreements or contracts with service providers contain provisions that the service providers will preserve the confidentiality of the customer information and that the information may only be used for the specific purpose of providing services and marketing on behalf of the Firm.

3) Limits on Sharing Account Number Information for Marketing Purposes. The Firm will not disclose, other than to a consumer reporting agency or excepted persons, an account number or similar form of access number or access code for a consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

4) Safeguarding Customer Records. In order to safeguard customer records and information, only Firm personnel that need to know the information to perform their job functions may access customer information. Personnel not required to know customer information are prohibited from accessing the information. The Firm and its personnel must take appropriate measures to ensure that customer information is kept confidential and secure in order to avoid unauthorized access, use or disclosure. These measures include, but are not limited to:

a) Firm personnel are prohibited from discussing customer information with anyone except with those persons who need to know such information.

b) Computers should be turned off or logged off when not in use, especially when the office is closed.

c) Passwords for computer access should be kept confidential and are not to be disclosed to any other person. If a member of the Firm has reason to believe that his or her password has been compromised, that individual should take immediate steps to change his or her password.

d) Computer passwords should be changed periodically.

e) Files and filing cabinets containing customer information should be kept secure and locked up when not in use.

5) Training and Supervision. The Firm will provide training to its personnel to educate them on the Firm's privacy policy as well as the procedures that should be followed to assure the confidentiality of customer information. At least on an annual basis, the Firm will require all personnel to sign an acknowledgement that they understand and have complied with the Firm's privacy policy and procedures (Refer to Attachment B). In addition, the Firm will periodically review or audit its privacy policy and procedures to assure ongoing compliance.

6) Obligation to Report. Any breach of the Firm's privacy policy or procedures must be reported immediately to the Firm's designated person. In addition, because of the importance of maintaining the privacy of customer information, any questions regarding the Firm's privacy policy and procedures should be directed to the designated person of the Firm.

State Privacy Requirements

Accordingly, the designated person shall determine for each state in which individual customers reside whether there are additional state law privacy requirements.

Massachusetts Privacy Law (201 CMR 17)

The Firm, and any other entity with customers or associated persons who reside in Massachusetts, is required to develop a separate comprehensive written information security program ("WISP"). The WISP sets forth the firm's procedure for evaluating their electronic, administrative and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of Massachusetts.

WISPs must:

1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
3. Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. Include safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00;
5. Include a process to regularly monitor the effectiveness of those safeguards.

All employees of the firm must receive and acknowledge receipt of the WISP. In addition, all employees must receive training on the WISP.

Nevada Privacy Law (NRS 603A)

The Firm, and any other entity with customers in Nevada, must develop policies and procedures that:

(i) Implement and maintain reasonable security measures to protect a customer's personal information from unauthorized access, acquisition, destruction, use, modification or disclosure; and
(ii) Require contracts for the disclosure of customer personal information to include a provision requiring the third party to implement and maintain reasonable security measures to protect a customer's personal information from unauthorized access, acquisition, destruction, use, modification or disclosure.

E) How the Firm Uses Information

The Firm may use personal information and nonpublic personal information that it collects or receives: (i) to respond to requests or questions; (ii) to communicate with a customer about the customer's relationship with the Firm; (iii) to improve the Firm's services and operations; (iv) for security, fraud prevention, and related protective purposes; and (v) as otherwise permitted by applicable law.

F) Data Security Specifics

In addition to the safeguards described above, the Firm uses reasonable technical and organizational measures designed to protect the confidentiality, integrity, and availability of information. Depending on the nature of the information and the relevant systems, these measures may include authentication, access controls, monitoring, auditing, and encryption. No method of safeguarding information is completely secure, however, and internet transmission is not always secure. Accordingly, the Firm cannot guarantee that its safeguards will be effective or that information transmitted over the internet will always be secure.

G) Retention of Personal Information

The Firm retains personal information for as long as reasonably necessary to carry out the purposes described in this Policy and to comply with applicable laws and recordkeeping requirements. Retention periods may vary depending on the nature of the information, the purposes for which it is used, and the Firm's legal and business needs.

H) Cross-Border and International Data Transfers

Information may be stored or processed in the United States. If a customer or user is located outside the United States, the customer's or user's information may be transferred to, accessed from, or processed in the United States or other jurisdictions where the Firm or its service providers operate. Those jurisdictions may have data protection laws that differ from those in the customer's or user's home jurisdiction. The Firm will handle transferred information in accordance with this Policy and applicable law.

I) Automated Decision-Making

The Firm does not engage in automated decision-making in processing personal information.

J) Children's Privacy

The Firm's services and, if applicable, any customer-facing website or online platform are intended for adults. The Firm does not knowingly collect personal information from children under 16. If a parent or legal guardian believes that a child under 16 has provided personal information to the Firm, the parent or legal guardian should contact the Firm's designated compliance contact.

K) Business Transfer

In connection with a merger, acquisition, sale of assets, or other business transfer, personal information may be disclosed to a potential or actual acquirer or other transaction party and may be among the assets transferred, subject to applicable law.

L) Links to Third-Party Sites

If the Firm operates a customer-facing website or online platform and it includes links to third-party websites or services, those websites or services are not controlled by the Firm. This Policy does not apply to their privacy practices. The Firm is not responsible for the content or privacy practices of third-party websites or services, and users should review the applicable privacy policies.

M) Cookies and Tracking Tools / Online Collection

To the extent the Firm collects information through a customer-facing website or online platform, it may use cookies, web beacons, and similar tracking tools to support functionality and collect information about visits to the website or platform. These tools may collect nonpersonal or technical information, such as an IP address, browser type, operating system, device information, the date and time of a visit, visit duration, and related usage data.

Where the Firm operates a customer-facing website or online platform, a user may be able to control or reject cookies through browser or device settings. Blocking or deleting cookies may affect functionality and may not stop all collection or tracking described in this Policy. Some



browsers or devices offer “Do Not Track” or similar signals; because those signals are not uniform, the Firm may not respond to them unless required by applicable law.

N) Policy Updates and Modifications

The Firm may modify, update, or otherwise revise this Policy from time to time. Any modification, update, or revision will become effective when the revised Policy is provided or otherwise made available by the Firm, unless a later effective date is stated or applicable law requires additional notice. The Firm will provide notice of material changes as required by applicable law.

O) Contact Information

Questions regarding this Policy or the Firm’s privacy practices should be directed to the Firm’s designated compliance contact: Mihai Prisacariu, +1 617 917 2605, mprisacariu@signalmarkets.com.