General Self-Examination Questionnaire for All Members

Registration

- Has the Member listed all of the following individuals as principals on the Member’s Form 7-R? (Registration Rules 208 and 101(t)):
  - Individuals who hold the following positions with the Member:
    - Sole proprietor of a sole proprietorship;
    - General partner of a partnership;
    - Director, president, chief executive officer, chief operating officer, chief financial officer or a person in charge of a business unit, division or function subject to regulation by the Commission of a corporation, limited liability company or limited partnership;
    - Manager, managing member or a member vested with the management authority for a limited liability company or limited liability partnership; or
    - Chief compliance officer.
  - Individuals who directly or indirectly, through agreement, holding companies, nominees, trusts or otherwise, have the following financial relationships to the Member:
    - Own 10 percent or more of the outstanding shares of any class of the Member’s stock, other than non-voting stock;
    - Are entitled to vote 10 percent or more of any class of the Member’s voting securities;
    - Have the power to sell or direct the sale of 10 percent or more of any class of the Member’s voting securities;
    - Have contributed 10 percent or more of a Member’s capital;
    - Are entitled to receive 10 percent or more of a Member’s net profits.
  - Individuals who have the power to exercise a controlling influence over an applicant’s or registrant’s activities that are subject to regulation by the Commission.

- Has the Member listed all of the following entities as principals on the Member’s Form 7-R? (Registration Rules 208 and 101(t)):
  - A general partner of a partnership;
  - The direct owner of 10 percent or more of any class of an entity’s securities, other than non-voting stock; or
  - Entities that have directly contributed 10 percent or more of a Member’s capital unless such capital contribution consists of subordinated debt contributed by:
    - An unaffiliated bank insured by the Federal Deposit Insurance Corporation;
- A United States branch or agency of an unaffiliated foreign bank that is licensed under the laws of the United States and regulated, supervised and examined by United States government authorities having regulatory responsibility for such financial institutions; or
- An insurance company subject to regulation by any State.

- Has the Member listed all branch office locations and branch office managers on the Member’s Form 7-R? (Interpretive Notice ¶9002)
- Have all branch office managers passed the branch office manager proficiency exam? (NFA Compliance Rule 2-7)
- Do all branch offices hold themselves out in the name of the Member? (CFTC Regulation 166.4)
- Has the Member listed on the Form 7-R or updated on the Form 3-R all “doing business as” names? (Registration Rules 204 and 210)
- Does the Member prohibit individuals who are not registered as associated persons (“AP”) from soliciting or accepting customer orders (except in a clerical capacity) or from supervising those individuals? (CEA Section 4k)
- If the Member terminated any principal’s, branch office manager’s or AP’s affiliation with the Member, did the Member file with NFA an Individual Withdrawal Notice (Form 8-T) within 30 days after the termination? (Registration Rule 214)
- Is the information provided on the Member’s Form 7-R still accurate and complete (including but not limited to names, addresses, phone numbers, e-mail addresses, etc.). If there were any changes that rendered the information inaccurate or incomplete, did the Member update and correct the information on NFA’s Online Registration System? (Registration Rule 210)
- Has the Member reviewed commission payouts and other disbursements to ensure that only NFA Members are being paid for customer business? (NFA Bylaws 301 and 1101)
- Does the Member review all parties it does business with to ensure those that are required to be registered are registered, and, if required to be an NFA Member, are NFA Members? (NFA Bylaw 1101 and Compliance Rule 2-36(d))
- If the Member and any of its Associates intend to engage in retail forex transactions, has the Member designated itself a forex firm and designated the Associate(s) a forex AP on NFA’s Online Registration System? (NFA Bylaw 301(j))

**Supervision** (NFA Compliance Rules 2-9 and 2-36, and Interpretive Notices ¶9019 and 9053)

- Has the Member designated a “compliance officer” who is responsible for handling customer complaints or inquiries of a compliance nature including matters received in branch offices?
• Does the Member have a compliance procedures manual or other written documentation that outlines the Member's policy with respect to handling compliance matters, such as customer complaints or inquiries?
• Does the Member have a systematic method of recording, investigating and responding to customer complaints or inquiries?
• If the Member has any branch offices or GIBs, does it have an Internal Audit Department or other designated individual ("Auditor") who monitors the branch offices and/or GIBs, including annual on-site inspections, using a written audit program?
  o Has the Auditor prepared a written summary of findings noted during an on-site inspection of a branch office or GIB and submitted the report to a partner or officer?
  o If the Auditor noted any problems during an on-site visit or other during other monitoring, has the Member taken appropriate corrective action?
• Does the Member have policies and procedures regarding the hiring and supervision of APs who have been or whose past employers have been disciplined by NFA or the CFTC for fraud?
• If the Member engages in retail forex, does the Member have procedures to screen prospective Associates to ensure that they are qualified and to determine the extent of supervision they will need if hired?
• Does the Member supervise sales solicitations by one or more of the following methods: direct listening, reviewing taped solicitations, silent phone monitoring and customer contact?
• Does the Member provide its APs with training on proper sales solicitations for transactions in the forex, futures and options markets?
• Does the Member distribute changes in rules or regulations to appropriate personnel?
• Does the Member monitor incoming and outgoing mail in order to intercept/identify any customer complaints?
• Does an officer or other supervisory personnel regularly review trading in non-customer and proprietary trading accounts?
• If the firm has had any traders with reportable positions, has it filed a Form 40 with the CFTC? (CFTC Regulation 15.02 and 15.03) If not, the firm must file this form immediately.

Ethics Training (NFA Compliance Rule 2-9 and Interpretive Notice ¶9051)
• Does the Member have policies and procedures regarding the ethics training requirements for APs, detailing areas such as content, frequency and format of training? For further assistance in drafting these ethics training procedures, see Appendix C on NFA's website.
- Have all of the Member’s APs received ethics training in accordance with the firm’s procedures? Has the Member maintained records documenting compliance with these procedures, including dates and providers of training and materials used or distributed?

- Does the firm use an ethics training provider (either internal or external) who is qualified to conduct training (e.g. has completed relevant proficiency testing and has three years of relevant industry experience, or similar experience)?

**Business Continuity and Disaster Recovery Plan** (NFA Compliance Rule 2-38 and Interpretive Notice ¶9052)

- Does the firm have a written business continuity and disaster recovery plan (BCDR) that outlines the procedures to be followed in the event of an emergency or significant disruption? (See Appendix B for assistance in drafting a BCDR plan)

- Does the firm test the effectiveness of its (BCDR) plan on a periodic basis or at least once a year and maintain evidence of that review?

- Does the firm update its BCDR plan as necessary to respond to material changes in the Member’s operations?

- Has a supervisory individual reviewed the plan and signed off that review?

- Has the firm distributed the BCDR plan to its key employees and communicated the essential components of the BCDR plan to all employees?

- Does the Member maintain copies of the BCDR plan at one or more off-site locations that are readily accessible to key employees?

- If an FDM or FCM Member, has the firm provided or updated NFA with the name and contact information for all key management employees? Has the firm provided NFA with the location, address and telephone number of its primary and alternative disaster recovery sites?

- If an IB, CPO, or CTA Member, has the firm provided or updated NFA with emergency contact information for one or more individuals NFA can contact in the event of an emergency? Are those individuals authorized to make key decisions in the event of an emergency?

**Account Opening** (NFA Compliance Rules 2-9, 2-10, 2-30 and 2-36)

- Does the firm obtain the following information from customers who are individuals: name, address, occupation or business description, estimated annual income, estimated net worth, age and prior investment and futures trading experience? For all other non-ECP customers: name, address, principal business, net worth or net assets and current estimated annual income (if not available the previous year’s annual income)?

- Does the Member require that the necessary information be obtained and recorded prior to permitting a new account to commence trading?
• If an account is opened in the name of an entity, does the Member obtain some type of authorization signed by appropriate personnel (such as a corporate resolution) indicating who has the authority to open and trade the account and identifying any account limitations?
• Does the Member require a partner, officer, director, branch office manager or other supervisory employee to approve a new customer account and document this review?
• Does the firm provide adequate risk disclosure to customers prior to opening an account?

Privacy Rules (CFTC Regulation 160 and NFA Compliance Rule 2-4)
• Does the firm have a written privacy policy pertaining to consumer financial information as required by CFTC Regulation 160? Does the firm provide the privacy notice to customers at the time the account is opened and where required annually thereafter?
• Does the firm provide and obtain customer “opt out” notices as required?
• For further assistance in drafting these privacy procedures, see Appendix D on NFA's website.

Promotional Material (NFA Compliance Rules 2-29 and 2-36)
• Does the Member have written procedures to supervise the preparation and use of promotional material?
• Does the Member require an officer, general partner, sole proprietor, branch office manager or other supervisory employee other than the individual who prepared the material to approve promotional material in writing before its use?
• Does the Member maintain all promotional materials and written approvals for a period of five years from the date last used?
• Does the Member maintain supporting documentation for all statements, claims and performance results?
• Does the firm ensure that the promotional material includes all material information necessary to ensure that it is not misleading?
• If the material mentions the possibility of profit including the presentation of profitable past performance results, does the Member include an equally prominent statement of the risk of loss?
• Does the Member calculate rates of return in a manner consistent with CFTC Part 4 Regulations?
• Does the Member ensure that any presentation of past performance of any actual accounts is representative of the actual performance of all reasonably comparable accounts for the same time period?
• Does the Member include a statement that past results are not necessarily indicative of future results when past performance is mentioned?
Does the Member ensure that statements of opinion are identifiable as such and have a reasonable basis in fact? Does the Member maintain support for such statements?

Does the Member ensure that the promotional material does not include any guarantee against loss?

Does the Member ensure that reprints of articles have been supplemented with the proper disclosures and disclaimers?

Does the Member include the hypothetical performance disclaimer prescribed by NFA Compliance Rule 2-29(c) with any hypothetical performance results? The Member must cease using hypothetical results when there are three months or more of actual trading results for the offered program.

When the Member uses hypothetical results for a trading system, does the Member also include either the actual results of all customer accounts directed by the Member for the past five years (or entire performance history if less than five years), or if the Member has less than one year of experience directing accounts, the results of any proprietary trading over the past five years (or the entire performance history if less than five years)?

Does the Member calculate hypothetical results in the same way as actual results?

When the Member uses both hypothetical results and actual results, does the Member ensure that the actual results and hypothetical results are appropriately identified, separately formatted, discussed in an equally balanced manner and calculated pursuant to the same rate of return method?

Does the Member explain all material assumptions made in preparing hypothetical results, including at least the minimum investment amount, distribution or reinvestment of profits, commission charges, management and incentive fees, and the method used to determine the purchase and sale price for each trade? (NFA Interpretive Notice ¶ 9025)

Does the Member submit all radio, television advertisements, audio podcasts and videos on the internet that make any specific recommendations or refer to or describe the extent of any profit obtained in the past or that can be achieved in the future to NFA’s promotional material review team for its review and approval at least 10 days prior to first use?

Does the Member prohibit the use of promotional material that contains any of the following below?

- Claims regarding seasonal trades;
- Claims regarding historical price moves;
- Claims regarding price movements that are characterized as conservative estimates when in fact such price movements would be dramatic;
- Claims using certain pricing data for a product different from the one being marketed in the promotional material;
• Claims containing profit projections;
• Claims containing “cherry picked” trades; and
• Claims regarding mathematical examples of leverage as a means of suggesting that prospective customers are likely to earn large profits from trading.

• Does the Member ensure employees and agents are not purchasing leads from non-Members required to be registered and/or using fraudulent advertising practices? Does the Member maintain a record of any non-member or member advertisement used?

• If the Member engages in retail forex, has the Member ensured that its promotional material does not represent any of the following below?
  o Forex funds deposited with an FDM are given special protection under the bankruptcy laws or that assets necessary to satisfy its obligations to customers are more secure because the Member keeps some or all of those assets at a regulated entity in the U.S. or a money center country. (NFA Interpretive Notice ¶ 9053)
  o Its services are commission free without prominently disclosing how it is compensated in near proximity to that representation. (NFA Interpretive Notice ¶ 9053)
  o It offers trading with "no-slippage" or that it guarantees the price at which a transaction is filled (unless it can also demonstrate that all orders for all customers have been executed and fulfilled at the price initially quoted on the trading platform when the order was placed and no authority exists, pursuant to a contract, agreement, or otherwise, to adjust customer accounts in a manner that would have the direct or indirect effect of changing the price at which an order was executed). (NFA Interpretive Notice ¶ 9053)
  o Solicits customers based on the leverage available unless the material balances any discussion regarding the advantages or leverage with an equally prominent contemporaneous disclosure that increasing leverage increases risk. (NFA Interpretive Notice ¶ 9053)

**E-Mails** (NFA Compliance Rules 2-9 and 2-29, and Interpretive Notice ¶ 9037)

• Does the Member have written procedures to review the use of futures-related e-mail by employees and agents, which identify by title or position the person responsible for conducting the review and address how and with what frequency e-mails will be reviewed, how that review will be documented and what type of e-mails will be pre-reviewed and post reviewed?

• Does the Member ensure e-mails are in compliance with NFA’s promotional material content and review procedures?
Websites and Social Networking Groups (NFA Compliance Rules 2-9 and 2-29, and Interpretive Notices ¶ 9037, ¶ 9053, and ¶ 9063)

- Does the Member have written procedures to supervise the preparation and use of websites?
- Does the Member require prior review and written approval of the website by an appropriate supervisor?
- Does the Member ensure the website meets the standards of content established in NFA Compliance Rule 2-29?
- Does the Member ensure paid hyperlinks to the firm’s website do not contain deceptive information regarding futures or options trading?
- Does the Member monitor the general content of any websites to which the Member links?
- Does the Member properly review personal websites or on-line social networking groups used by employees or agents to attract business for the firm?
- Does the Member monitor blogs, chat rooms or futures or forex-related forums hosted by the firm or its Associates and take down any misleading or fraudulent posts and ban users for egregious or repeat violations?

Cybersecurity (NFA Interpretive Notice ¶ 9070)

National Futures Association (“NFA”) has developed the following questionnaire to assist firms in meeting their obligations under NFA’s Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49 entitled Information Systems Security Programs (Cybersecurity Notice). The Cybersecurity Notice adopts a principles-based risk approach to allow Member firms some degree of flexibility in determining what constitutes “diligent supervision,” given the differences in Members’ size and complexity of operations, the make-up of customers and counterparties serviced by Members, and the extent of Members’ interconnectedness. NFA recognizes that a one-size-fits-all approach will not work for the application of these requirements. However, the Cybersecurity Notice does require each Member to adopt and enforce an information systems security program (ISSP) appropriate to its circumstances.

The firm must develop and maintain a written ISSP for securing customer data and access to their electronic systems, which should be maintained with the rest of the firm’s written procedures. Although the firm is not required to have a separate single document describing every aspect of its ISSP, a comprehensive written policy may be the best way to ensure that firm personnel know what the firm’s policy is, depending upon the firm’s size and complexity of business and technological operations. Similarly, while the ISSP may be implemented at an
enterprise wide level, the ISSP should be appropriate to the Member’s information security risks. This is important because just having a policy is not enough to meet your regulatory requirements. You must also implement and follow that policy and review it at least annually to keep it current and complete.

The questions listed below are very general and do not cover every aspect of the Cybersecurity Notice, which you should consult when designing your ISSP. The questions are intended to provide a tool or process to assist you in developing the written ISSP. The firm should also consider whether it has the internal expertise to develop and implement a written ISSP or whether additional resources are needed either through hiring cyber professionals or engaging consultants with the necessary expertise.

You should complete this questionnaire as appropriate in light of your firm’s size and complexity of operations, the make-up of your customers and counterparties, and the extent of your interconnectedness. You should carefully consider the firm’s operations before deciding that a particular point is not applicable.

**Identification of threats and vulnerabilities:**

**Taking an inventory of information assets**

- Has the firm taken an inventory of the data and information that the firm creates, collects, receives, uses, processes, stores, or communicates to others?

- Has the firm identified the systems, networks and processes by which such data is created, collected, received, used, processed, stored, or communicated?

- Has the firm identified where in the firm (e.g., which office and which department), the data and systems are located, and who controls them?
  
  - Has the firm identified all data privacy or data security laws that apply to the information collected, processed, and stored?
  
  - Does the firm have data that is in the possession and control of a third party, such as an outsource service provider, back-up facility provider or cloud storage provider?
Does the firm provide third-party service providers with access to its data and systems?

**Conducting a risk assessment**

A risk assessment identifies threats and vulnerabilities to the information assets used by the company and assesses the potential impact/harm that would result if a threat materializes. Threats include, for example cyber or physical attacks; human errors; disasters, accidents, and failures beyond the control of the organization, such as a fire, flood, or tornado. A vulnerability is a flaw or weakness that could be exploited by a threat e.g., unrestricted access to the firm's premises where information systems hardware is located, a system with easy to guess passwords, unencrypted data on a laptop computer or disgruntled or poorly trained employees.

- Has the firm identified the reasonably foreseeable internal and external threats to the information and system assets?
- Has the firm identified the vulnerabilities that could be exploited by threat sources?
- Has the firm assessed the likelihood that the identified threats will materialize, and if so, the probability that it will exploit one or more of the vulnerabilities to cause harm?
- Has the firm evaluated the potential damage that will result in such case?
- Has the firm assessed the sufficiency of the security controls in place to guard against the threat?

**Deployment of protective measures against the identified threats and vulnerabilities:**

**Physical Security**

- Has the firm considered and, when appropriate, implemented restrictions on physical access to:
  - the premises where its information systems are located; and
  - the data processing equipment used for storing, accessing and processing data?

- Has the firm considered and, when appropriate, implemented measures to:
o protect against power interruptions and other potential physical hazards such as water and fire damage;

o restrict access to specific types of digital or printed information only to authorized users;

o securely store removable media, such as USB drives and CD/DVDs;

o secure the information on equipment and removable media that are taken out of the premises; and

o securely destroy and dispose of digital and printed information?

Technical Security

Access

• Has the firm considered and, when appropriate, implemented measures to:

  o prevent unauthorized persons from accessing information systems and data;

  o limit and control the scope of access by authorized users to information systems and data; and

  o authenticate and identify authorized users?

System Acquisition, Configuration and Change Management

• Has the firm considered and, when appropriate, implemented measures to:

  o with respect to third-party service providers, to the extent practical:

    ▪ conduct reasonable due diligence on third-party service providers that possess, control or have access to the firm's data or information systems;

    ▪ include contractual provisions in contracts with these third-party service providers requiring appropriate information security practices; and

    ▪ monitor the performance of these third-party service providers with respect to information security practices?

  o include appropriate security practices into the design and implementation of information systems;

  o test and evaluate the security of new systems;

  o verify that the system and software configuration are appropriate from a security perspective; and

  o ensure that system modifications are consistent with the firm's security program?

System and Information Integrity
- Has the firm considered and, when appropriate, implemented measures to:
  - protect against unauthorized changes to software;
  - protect information from unauthorized access, alteration, disclosure or destruction through, for example encryption of data; and
  - prevent the introduction of and protect against the effects of malicious software, e.g., viruses, etc.?

Data Movement

- Has the firm considered and, when appropriate, implemented measures to:
  - prevent unauthorized persons from moving data outside of the premises;
  - establish when, by whom and to whom sensitive data is transmitted; and
  - protect the confidentiality and integrity of data in the process of transfer or transmission through encryption?

Maintenance

- Has the firm considered and, when appropriate, implemented measures to:
  - identify, test and install software patches in a timely manner;
  - remove data from equipment that is sent off-site for repair and verify hardware and software security features functionality when the equipment is returned; and
  - approve, control and monitor remote maintenance activity?

System Activity Monitoring and Audit Records

- Has the firm considered and, when appropriate, implemented measures to:
  - determine whether continuous auditing of access to and alteration, deletion and copying of sensitive data is required;
  - identify the events which require auditing if auditing is not continuous; and
  - determine the content of audit logs?

Personnel

- Has the firm considered and, when appropriate, implemented measures to:
  - verify that its employees and service providers are technically qualified and are sufficiently trustworthy to access information systems containing sensitive data; and
  - specify the security obligations of its employees and service providers who have access to information systems containing sensitive data?
• Has the firm implemented information security training that
  o is appropriate based upon the employees' roles; and
  o is conducted for all employees upon hire and periodically thereafter?

Detection of Threats in a Timely Manner

• Has the firm deployed tools, techniques and procedures to:
  o monitor log-in attempts and report discrepancies;
  o detect actual and attempted attacks on or intrusions into the firm's information systems; and
  o identify unauthorized users

• Has the firm considered and, where appropriate, installed intrusion detection software that detect and reports unauthorized access to or actual or attempted installation of malicious software on the firm's information systems?

Response to Events that Threaten the Security of Electronic Systems

• Has the firm developed an Incident Response Plan (IRP) in the event of a security incident that identifies the team of people who are responsible for implementing the IRP and that contains procedures:
  o for timely notification of appropriate firm personnel and external parties;
  o to obtain the appropriate internal and external support to handle and report security incidents to regulatory and law enforcement authorities and persons or business partners whose information may have been compromised;
  o to take timely action to contain and recover from the security incident;
  o to document the date, time, nature and impact of and response to the security incident;
  o for training of the IRP team; and
  o for periodically testing the IRP to determine its effectiveness and document the test.

Recovery from the Events

• Has the firm integrated its ISSP with the firm's business continuity/disaster recovery plan?

Training

• Has the firm internally developed and implemented or contracted with a qualified service provider to provide an information security training program that
is designed to provide an understanding of the firm's ISSP and limit human error;

includes training for employees upon hiring and periodically thereafter appropriate to its employees' access to or involvement with its information systems; and

includes training topics such as social engineering tactics and other general threats that could compromise the firm's information system or result in data loss/breach?

**Annual Review of ISSP**

- Has the firm implemented a process to monitor the effectiveness of its ISSP at least on an annual basis?

- Has the firm considered whether its internal staff has the appropriate knowledge and training to perform the annual effectiveness review and, if not, engaged a qualified service provider to perform the review?

- Has the firm considered whether, based on the firm's size, business, technology, electronic connectivity with other entities and the potential threats identified in the firm's risk assessment whether to perform penetration testing of its information systems?

- Does the firm's ISSP effectiveness review include a process of remediating issues identified by the review?