



# FUTURES INDUSTRY ASSOCIATION

INC.

2001 Pennsylvania Avenue N.W. • Suite 600 • Washington, DC 20006-1807 • (202) 466-5460  
Fax: (202) 296-3184

November 15, 2001

Ms. Kathryn Camp  
Associate General Counsel  
National Futures Association  
Suite 1600  
200 West Madison Street  
Chicago IL 60606

**Re: Interpretative Notice Regarding Automated Order Routing Systems**

Dear Ms. Camp:

The Futures Industry Association (“FIA”) welcomes this opportunity to comment on the National Futures Association’s (“NFA’s”) proposed Interpretative Notice Regarding Automated Order Routing Systems, which was released for comment on August 31, 2001 (“Notice”). FIA is a principal spokesman for the commodity futures and options industry. Our regular membership is comprised of approximately 50 of the largest futures commission merchants (“FCMs”) in the United States, each of which is also a member of NFA. Among our associate members are representatives from virtually all other segments of the futures industry, both national and international. Reflecting the scope and diversity of our membership, FIA estimates that our members effect more than 90 percent of all customer transactions executed on US contract markets.

FIA is pleased to support NFA in its efforts to develop general standards for automated order routing systems. As the self-regulatory organization for the US futures industry, with particular responsibility for the protection of commodity futures market participants, providing such guidance to its members is certainly an appropriate role for NFA. However, as discussed in greater detail below, FIA believes that the proposed Notice is far too prescriptive.

We recognize that the Notice states that “other procedures besides the ones described in this Interpretative Notice may comply with the general standards for supervisory responsibilities.” Nonetheless, the Notice goes on to advise members that, among other technologies and procedures: (1) the system *should* use encryption for all authentication; (2) firewalls *should* be used; (3) members *should* conduct periodic testing of the security of the system; and (4) the member *should* use redundant systems. [Emphasis supplied.] The Notice concludes with the warning that “NFA Compliance Rule 2-9 requires NFA Members to meet the standards for security, capacity, and credit and risk controls that are set out in this Interpretative Notice.” Members that fail to do so presumably could be subject to a disciplinary proceeding.

FIA strongly believes that any guidance NFA provides should be general in nature to allow firms the flexibility to adopt standards that are reasonable designed to address their business needs. We

are concerned that an unintended consequence of the Notice in its present form is that members electing to adopt procedures different from those set forth in the Notice would bear a greater burden in subsequent SRO audits in establishing the adequacy of their supervisory procedures. Such member firms would have a similar burden in any judicial proceeding or arbitration brought by users of automated order routing systems.

For these reasons, and subject to our comments below, FIA strongly recommends that NFA recast the Notice as a general guideline, without specifying particular standards and technologies that members should consider in developing supervisory procedures with respect to automated order routing systems.

### **General Comments**

In preparing this comment letter, FIA reviewed a number of documents published by various US securities regulatory authorities, the International Organization of Securities Commissions (“IOSCO”) and the General Accounting Office (“GAO”) that appear to be relevant to the issues discussed in the Notice.<sup>1</sup> However, none of these documents appears to mandate the detailed requirements that implementation of the Notice would impose on members. To the contrary, these documents are more narrowly focused, emphasizing in particular the obligation of broker-dealers to assure the operational capacity of their systems and to provide adequate disclosure to their customers concerning the risks of trading through such systems.

For example, in Staff Legal Bulletin No. 8, the SEC staff only “seeks to emphasize to broker-dealers the importance of having adequate capacity to handle high volume or high volatility trading days, and conducting capacity planning on a regular basis.” NASD reinforces this guidance in Notice to Members 99-11 and Notice to Members 99-12. The IOSCO report states that regulators “*may wish to consider* whether online brokers, as a matter of business interest, legal requirements or regulatory guidance, are prepared to address risks relating to system capacity, resilience and security” by addressing several issues, including certain of those discussed in the Notice. [Emphasis supplied.] However, the report makes no definitive recommendations in this regard.

Only the OCIE Report discusses matters such as encryption, firewalls and passwords. However, the OCIE Report does not purport to require all broker-dealers to employ such techniques to assure the security of their systems. It simply describes current practices and makes

---

<sup>1</sup> (1) Securities and Exchange Commission (“SEC”) Staff Legal Bulletin No. 8 (MR), September 9, 1989; (2) SEC Office of Compliance Inspections and Examinations (“OCIE”): Examinations of Broker-Dealers Offering Online Trading: Summary of Findings and Recommendations, January 25, 2001; (3) SEC Notice of Proposed Rulemaking, Operational Capability Requirements of Registered Broker-Dealers and Transfer Agents and Year 2000 Compliance, March 11, 1999; (4) GAO Report on On-Line Trading, July 20, 2001; (5) National Association of Securities Dealers (“NASD”) Notices to Members 98-66, 99-11 and 99-12; New York Stock Exchange (“NYSE”) Notices to Members 89-6, 92-15 and 92-43; and (6) IOSCO Internet Task Force Report on Securities Activity on the Internet II, June 2001.

recommendations with respect to issues that broker-dealers offering on-line trading should consider. The OCIE Report, therefore, contrasts sharply with the Notice, which advises members that “NFA Compliance Rule 2-9 requires NFA Members to meet the standards for security, capacity, and credit and risk management controls that are set out in this Interpretative Notice.”

### **Specific Comments**

**Written Supervisory Procedures Generally.** In general, FIA agrees with NFA that member firms should have special written supervisory procedures governing their business activities. Nonetheless, we do not believe that written supervisory procedures are required when appropriate safeguards are built into the automated order routing system itself. This latter approach would be consistent with that of the NYSE in its releases. We recommend that the Notice be revised accordingly.

**Security: Authentication, Encryption and Firewalls.** FIA agrees that members that accept orders should have procedures in place reasonably designed to protect the reliability and confidentiality of orders and account information during the order routing process. The choice of appropriate procedures, however, should be left to each member. Authentication methods, encryption and firewalls may describe the more obvious means of assuring security of a system that may be available currently. However, it is by no means clear that these procedures are always available or that they should be mandatory for all member firms regardless of their size, structure or type of business. Moreover, as NFA has recognized, technology is constantly evolving. Members should not be locked into using encryption and firewalls, for example, if more appropriate and effective security procedures are developed or identified. Finally, we oppose the proposed requirement that a warning be generated if a firewall is breached. We believe that the current technology is too imprecise in distinguishing actual breaches of firewalls that threaten the security of a system from other events.

**Security: Authorization.** FIA strongly objects to the proposed requirement that members “should periodically check each customer to verify that the individuals authorized by the customer to access the AORS are still authorized to do so and discover whether any passwords (or other forms of authentication) should be disabled.” This proposed requirement unnecessarily and unfairly shifts the burden of responsibility in this regard from the customer, where it rightly belongs, to the member firm. This requirement would also contradict many customer account agreements, which clearly place responsibility with the customer to advise the member firm whenever a change is made in the identity of individuals authorized to enter trades on behalf of the customer or the security of passwords has been compromised.

**Security: Periodic Testing.** FIA also strongly objects to the requirement that member firms conduct “periodic testing of the security” of the order routing system using independent audit departments or qualified third parties. Internal audit departments do not necessarily have the expertise to conduct such tests. For example, if a member firm uses order routing systems developed by third parties, senior staff in the member firm’s systems department may be the most qualified and in the best position to evaluate the third party developed software for security measures. Moreover, third parties with the necessary technical expertise to test these systems are few and are likely to be expensive. FIA suggests that a member firm be required only to review periodically the security procedures for its system.

**Security: Administration.** The responsibility for assuring the security of an order routing system rests with the firm and not a single individual. It is the member firm’s responsibility to determine the number of people who should be responsible for the security of the member’s system. It is not necessary or appropriate to require that one individual be held responsible.

**Capacity: Disaster Recovery and Redundancies.** FIA agrees that a member firm should have contingency plans reasonably designed to service customers if a system fails. However, it is not appropriate to require a member firm to use a redundant system or to be able to convert to other systems if the need arises. Such a requirement could impose a significant financial and operational burden on member firms. What happens in the event of a system failure is properly a matter to be discussed between the member and the client. Additionally, any back-up procedures the member makes available to its customers are reasonable in view of the member’s size, structure and type of business.

**Capacity: Advance Disclosure.** A member firm should not have to disclose in advance every factor that could possibly affect the system’s performance. It should be sufficient to highlight the material factors. Again, the more important point is that a member firm should adequately describe the procedures the customer should follow in the event of a system failure.

**Credit and Risk Management Controls: Pre-Execution and Post Execution Controls.** Provided it is clear that the decision whether to impose pre-execution or post-execution controls remains with the member firm, FIA does not object to this standard. Nonetheless, we understand that the systems intended to permit a firm to impose pre-execution controls are not well developed. In particular, complex trading strategies involving options are not well suited for pre-execution control processes. Similarly, the requirement with respect to post-execution controls appears to assume that a member firm will always be able to monitor trading “promptly.” This is not always possible, especially where the customer may execute a portion of its transactions through the telephone or through an executing broker. These trades are not taken into account by an automated order routing system, and often are not seen electronically on trade date. Separately, FIA agrees that firms should consider “fat finger” controls for certain customers. However, it is also important to note that, in many systems, the customer has the ability to override such controls.

**Credit and Risk Management Controls: Direct Access Systems.** We object to the proposed requirement that member firms use pre-execution controls whenever a customer is allowed to use a direct access system that does not allow a member to monitor trading promptly. We agree that a member firm should consider whether to impose such controls. However, that decision, which is a business decision, should rest with the member firm. It is also important to note that certain exchange-provided terminals do not permit carrying firms to impose pre-execution controls. Moreover, exchanges are providing the API interfaces to order routing vendors that do not provide pre-execution control ability. These vendors often market their systems directly to the end-users. FIA recognizes that Notice provides that a member is not responsible for a system chosen by the customer, including systems provided by exchanges. Nonetheless, within the same sentence, NFA states that the member “is nevertheless responsible for adopting procedures reasonably expected to address the trading, clearing, and other risks attendant to its customer relationship.” NFA should first address this issue directly with the exchanges and not the member firms. Any exchange-sponsored systems should include these controls, which enhance the integrity of the entire system.

### **Conclusion**

For all of the above reasons, FIA does not believe that that Notice should be adopted in its present form. Rather, we believe the Notice should be substantially rewritten and published as a guideline, describing issues that member firms should consider in connection with implementing reasonable supervisory procedures governing the use of automated order routing systems by their customers. We would be pleased to work with NFA to this end.

Sincerely,

John M. Damgard  
President

cc: Daniel J. Roth, Senior Executive Vice President  
Thomas W. Sexton, General Counsel