BEFORE THE
NASD AND THE NYSE
WASHINGTON, D.C. 20006-1506

In the matter of the Proposed Joint Guidance Regarding the Review and Supervision of Electronic Communication Comment Period Expires: July 13, 2007	)	Joint Request for Comment

---

COMMENTS OF ORCHESTRIA CORPORATION

Orchestria Corporation, as the premier provider of Electronic Communication Control to the financial and trading industry, welcomes the opportunity to provide comment upon the NASD and NYSE's Proposed Joint Guidance Regarding the Review and Supervision of Electronic Communications ("Joint Request for Comment"). The recognition by both the NASD and the NYSE of the impact that electronic communication has upon members is both correct and comforting, as it re-emphasizes the role and leadership offered by these regulatory organizations. Rather than attempting to limit or forbid the use of communication technologies, both the NASD and the NYSE recognize that empowering, rather than inhibiting, is the appropriate method for balancing business and regulatory needs. To that extent, Orchestria agrees and applauds the commitment by the NASD and the NYSE to provide guidance for targeted supervision and technological controls that more reflects the spirit of the regulations to protect the public, the members, and the industry as a minimum basic requirement for electronic communication supervision.

As recognized in the Joint Request for Comment, electronic communication supervision and review can no longer be a simple "review 100% of everything that goes out" process because of the volume of daily electronic activity and the significance of the content thereof. Instead, it is well established in the

proposed guidance that companies are compelled to use "risk-based" systems for determining what communications should and must be reviewed. The Joint Request for Comment allows that this can be accomplished through the use of lexicon-based systems and random review; however, our experience in analyzing the data of customers who have previously used such solutions has made clear than neither of them — whether used independently or in concert — is sufficient. What we have found is that these solutions generate an unreviewable number of alerts, thereby insuring that most problems will never be identified. In essence, our clients were faced with finding the proverbial needle in a haystack with little or no hope of ever doing so.

As noted above, from an objective and demonstrable point of view, pure lexicon-based and random review methodologies are measurably ineffective with respect to identifying communications of concern. Lexicon solutions can generate alert rates of 60% or more, making it nearly impossible for an organization to individually view and assess each communication since many of the members generate more than 1 million messages each day. Likewise, random sampling, while reducing the alert rate to a fixed percentage, creates the statistical probability that communications of concern will never be seen. First, if a business randomly samples only 5% of its emails, it will statistically be able to find only 5% of any violations that exist — i.e., it will be guaranteed to miss 95% of the items about which it is concerned. Second, where the number of "problem" emails is exceedingly small (e.g., single or double digits out of millions of e-mails), the likelihood that any of them will ever be identified by a reviewer with random sampling approaches zero percent (0%). Third, the members are disincentivized under this model to raise any issue because they know it is only the 'tip of the iceberg' and there is significant burden in trying to investigate how big a problem may be.

Businesses can begin to close this "effectiveness gap" by moving toward targeted post-event analysis, which generates alerts from multiple policies that are specifically targeted to identify violations of a particular nature, e.g., customer complaints, social security numbers or account information leaving the firm, gifts and entertainment, inside information sharing, communication across an internal information boundary, bribery, etc. Targeted post-event analysis policies place keywords into context,

which is analyzed through the examination of such factors as word frequency; word proximity; email metadata; attachments' presence, absence, and content; etc. Lexicon based systems are unable to compete with the accuracy of such a system because their methodology constitutes an "all-or-nothing" proposition, lumping all lexicon potentially indicative of many potential types of violations together and generating an overwhelming volume of irrelevant "noise". This usually forces a firm to sample this huge volume of "flagged" messages and dramatically reduces the original effectiveness of the lexicon based supervision system. Random sampling is statistically less effective because it is just that — random; yet violations do not occur on a random basis or of a frequency that would lead to identification through random sampling means. By implementing targeted post-event analysis, businesses can avoid the unreliable scatter-shot approach of random sampling, as well as the unreviewable over-inclusiveness of lexicon-based systems.

Take for example the topic of Gifts & Entertainment. As we have found from our field experience, lexicon-based keyword systems generate alert rates upwards of 38% with respect to that topic; if an advanced lexicon system is used, the alert rate can still be as high as 20%. Consequently, at a company that processes 1 million e-mails a day, anywhere from 200,000 to 380,000 alerts will be generated — a number that exceeds that of the company's ability to review. Post-event targeted review, like that offered by Orchestria, however, reduces that alert rate dramatically. In an actual deployment, Orchestria's Intelligent Review solution generated only 202 alerts out of 1 million messages, affording reviewers the opportunity to be properly assess all of the potential violations. To attain complete oversight, however, businesses must go even further because while it will have the ability to discover the loss of data by using post-event analysis, the damage has already been done. It cannot "un-ring the bell", so to speak.

What any business needs, what the members need, to ensure they conduct meaningful supervision and review of their electronic communications, protect the public interest, and effectively manage reputational, financial, and litigation risk, is a targeted surveillance system, with both pre-event and post-event analysis capabilities, and appropriate controls. Outside of the enormous burden of 100%

pre-send human review, only a "policy-based" system, that intelligently analyzes and actively controls all electronic communication, can be measurably effective at ensuring compliance in line with the intent of the regulations. Anything less reflects, at its core and for all intents and purposes, a failure to supervise completely.

Control-free message, web and file activity has been a particularly relevant topic for organizations that have failed to employ appropriate internal and external electronic information and activity controls. Last week alone, three major organizations were the victim of uncontrolled electronic action including: Boeing, where sensitive data was leaked by a former employee; Whole Foods, where the CEO posted questionable comments on Yahoo stock market forum; and Fidelity National Information Services Inc., where an administrator stole and sold in excess of 2.3 million bank and credit card records. Although these incidents occurred outside of the financial services industry, they could just as easily have occurred to any member; we have chosen not to use public examples of incidents among the members so as to avoid the appearance that any indictments were being made as a result.

The substantial and measurable difference in the results realized by use of a system like Orchestria's Intelligent Compliance solution and that of lexicon/sampling solutions provides ample proof that the Orchestria solution has a current ability to meet current industry needs and establishes a watermark for reasonably ensuring compliance with regulations and laws that few, if any, supervisory systems achieve. It is not often that available technology has the ability to keep current with the rules and regulations that are promulgated. Nevertheless, the technology exists. The technology's effectiveness has been proven in the field time and again. It is also equally rare, when such technology comes along to dramatically improve a member's effectiveness in ensuring compliance with the applicable regulations and laws, that the technology also reduces both the cost and burden of compliance. However, this in fact is the case with Orchestria's Intelligent Compliance solution. We invite further inquiry by the regulators and members into the set of capabilities we offer that would allow the members to implement every element of the proposed guidance. We also would further invite inquiry

into how the same platform may assist your members with other regulatory requirements in the areas of records management, legal hold, and information security.

In conclusion, Orchestria again applauds the forward direction and leadership that the NASD, the NYSE, and the members have shown, and continue to show, on the issue of ensuring compliance. It has been our pleasure to support this industry for the past four years in conducting meaningful supervision and we look forward to continuing to support the. Orchestria is proud to offer technology that provides measurably greater effectiveness while dramatically reducing cost and burden on the member organizations. We look forward to continuing to meet the challenges presented by an ever changing landscape of risks the members face and fully intend to remain an active participant in the continuing conversation on Electronic Communication Control.

Respectfully submitted,

Orchestria Corporation
437 Madison Avenue
New York, NY 10022

_____
David Cohen
Senior Vice President, Global Solutions

Dated: July 13, 2007