

Client Alert

SEC Fines Investment Bank For System Failures

On May 9, 2007, the SEC brought an administrative proceeding against a large investment bank alleging that the firm embedded undisclosed mark-ups and mark-downs in certain OTC executions and delayed execution of other orders, thereby not providing best execution to its retail customers.¹ The SEC alleged that the firm was reckless in improperly programming its automated OTC market-maker system, which caused the errors. Without admitting or denying the allegations, the firm agreed to pay a civil monetary penalty of \$1.5 million and disgorgement plus interest of approximately \$6.4 million. The firm also agreed to retain an independent compliance consultant to conduct a comprehensive review and provide recommendations on its automated retail order handling system.

In announcing the decision, Elaine Greenberg, Associate Administrator of the SEC's Philadelphia Regional Office, stated that ***"You can't blame it on the computer. The message in this case is to put brokers on notice that the commission is going to be looking at automated systems..."*** This is the latest in a series of SEC and SRO disciplinary actions where the regulators have imposed large penalties on various broker-dealers for failure to properly program and monitor automated systems.² Through these actions, the regulators have served notice on the industry that they will hold broker-dealers liable for systemic failures even when there is no intentional wrongdoing, and in some cases, no underlying violation other than the control failure itself.

With the increasing complexity of the trading markets and the volumes and speed at which securities trade in those markets, most firms have little hope of complying with regulatory requirements without sophisticated order management, trading and sales systems. Firms must diligently manage the development, implementation and maintenance of technology to assure compliance with regulatory requirements. Also, they must periodically review and test existing systems and technology to assure continued compliance. In essence, good supervision and good compliance now require even better technology and stronger IT control.

As a result, firms should periodically review and enhance existing IT control programs, or create new programs, to effectively manage systemic risk. There is no one size fits all solution to this problem. The programs must be tailored to the specific needs and risks of each firm's business. At a minimum, however, the following key principles, which can be gleaned from the recent cases, should be considered when enhancing or establishing such a control program.

¹ *In re Morgan Stanley & Co.*, Securities Exchange Act Release No. 55726 (May 9, 2007).

² See, e.g., *In re Morgan Stanley & Co. and Morgan Stanley DW Inc.*, Securities Exchange Act Release No. 54047 (June 27, 2006); *In re Instinet, LLC and INET ATS*, Securities Exchange Act Release No. 52623 (October 18, 2005); *In re Merrill Lynch, Pierce, Fenner & Smith Incorporated*, NYSE Exchange Hearing Panel Decision 05-27 (March 7, 2005); *In re SG Cowan LLC, et al.*, NASD Disciplinary Action (October 4, 2005).

1. **Identify the specific persons responsible for supervision of technology.** In many cases, this is not easy. Front line supervisors are generally not trained or sophisticated in technology. As a result, they usually defer to the IT Department to develop, implement and maintain systems. Staff in the IT Departments are generally not registered supervisors and do not have the same ongoing management responsibility for the business activities. While the firm's compliance department may play a significant role in the overall control process, it generally will not be deemed to be the supervisor of the systems. Nonetheless, identifying clear responsibility for systems and technology is critical. One solution could be joint responsibility through a committee of business, IT and compliance professionals with a clear reporting line to the head of the business unit.
2. **Obtain senior management support and allocate appropriate resources to the program.** An IT control program will not work unless it is fully supported by the senior management of the firm and proper resources are allocated to the program. Additional staff time in IT, compliance and business will be needed to make sure that this program works correctly. Appointment of an overall coordinator may be necessary to run the program. Senior management must be willing to stand behind the process and require compliance even if this would impose delays or additional costs on critical development projects. Without this support, the program will not have the "teeth" to succeed.
3. **Implement clear and practical written policies and procedures.** A written document should clearly articulate the policy, the process to be followed in obtaining approvals, and the consequences for failure to comply. The process should not be overly burdensome, however, as to tie up or limit technological development and innovation. Instead, the process should establish reasonable checkpoints and assign responsibilities that can reasonably be executed within the context of ongoing business. Again, adequate resources are necessary to assure that any review process is done in a timely and efficient manner.
4. **Consistently apply the policy to all systems and all technology.** The policy must be applied to all systems and to all technology development to be effective. If not, the process will be more of sieve than a safety net. Of course, flexibility can be built in based on the nature of the systems and the proposed development or change as long as the essential control elements of the program are met.
5. **Involve the compliance department in the early planning and development of new technology.** Early involvement of compliance will assure that the process works more smoothly and that no major problems develop at the last minute. If compliance and regulatory concerns are identified early, they can be dealt with in a timely and efficient manner, and built into the initial programming. On the other hand, if IT developers wait until the last minute to obtain compliance signoff, there could be substantial delays in the roll out of the technology. In the worst case scenario, a complete re-design of the technology may be necessary.
6. **Require formal compliance signoff.** It is essential to have a formal signoff process that is well documented before final implementation of new technology. This will protect the firm and individual employees from potential liability by establishing evidence of a reasonable process.
7. **Institute a change control process.** Compliance signoff for significant changes to systems is also essential, since many programming errors take place after initial implementation of technology. The challenge is identifying the changes that need to be reviewed. The firm should take a conservative approach requiring compliance review and approval whenever a change has the potential of impacting regulatory or compliance issues. This should be balanced against overburdening routine updates and changes.

8. ***Establish a rigorous test environment.*** Thorough testing of both new technology and significant changes to existing technology is critical before implementation to avoid potential problems. Compliance and regulatory requirements should be imbedded in this process.
9. ***Establish a periodic audit program of existing systems.*** Systems should be reviewed and tested on a periodic basis to assure that they continue to be in compliance with all regulatory requirements. The schedule of testing can be based on the complexity and risk of the individual systems. The regulators have repeatedly stated that systems cannot be allowed to run on autopilot and that firms need to “kick the tires” occasionally to make sure they are still running correctly.
10. ***Document the entire process.*** The entire process should be thoroughly documented to show regulators, internal and external auditors, and senior management of the firm that the process has been followed. While this does not always work as a complete defense to adverse actions, it goes a long way in showing that the firm had reasonable procedures in place to manage this risk and followed those procedures. Failure to follow existing procedures is one of the clearest paths to a disciplinary action.

* * * * *

May 22, 2007

For Additional Information

This client alert can be found, together with other recent Chadbourne & Parke LLP client alerts, on our website at www.chadbourne.com/publications. Our client alerts are for general informational purposes and should not be regarded as legal advice. If you have any questions regarding this alert, please contact any of the following:

New York

Gerard Citera

+1 (212) 408-5176

gcitera@chadbourne.com