Reprinted from THE WALL STREET JOURNAL.

WEDNESDAY, JANUARY 21, 2004

The Ultimate Insiders

By Howard Kalt

As we reflect on the spectacle of Martha Stewart striding into a Manhattan courthouse, investors should note that it's not just celebrities and corporate bigwigs whose trades attract the scrutiny of watchdogs. And although many believe their trades will be too small to get noticed, Ms. Stewart's sale of just one-tenth of 1% of the 7.7 million Imclone shares traded on Dec. 27, 2001, proves just the opposite. Relatively small fish—lawyers, commercial printers, consultants, spouses, children and friends of "tipsters"—have been caught, fined, humiliated and prosecuted.

One lower-profile case found a CFO's wife advising her adult children to buy prior to a planned acquisition, then sell as the agreement fell through—both times prior to public announcements. Others have included a financial printer who deciphered the code names being used in merger documents he was printing, an aerospace company executive's psychotherapist trading on patient discussion of an upcoming merger, and an investor relations consultant making several small trades in client stocks and later telling the SEC she had no inside information. Even international borders have failed to protect violators. The SEC froze $425,000 in stock and profits when Swedish stockbrokers bought a U.S. company's shares just prior to announcement of its purchase by a Swedish firm.

How are trades by such people uncovered? It's a lot easier than they realize. Each stock exchange devotes significant resources to identifying violators. For example, 560 people—a third of the NYSE's staff—work in the Regulation Division, which includes a Stock Watch Unit. The American and Nasdaq stock exchanges have similar units. All work closely with the SEC and, at times, the Justice Department. In addition, regulators can pay a 10% bounty for insider-trading tips, while the FBI uses a hotline and Web site to gather information.

The big weapon employed by the exchanges is technology. Computer modeling and data analysis software build an individual trading profile for each stock. Trading is monitored for both unusual activity prior to major announcements and unexplained stock price and/or volume fluctuations. At this point, Artificial Intelligence, the science of computer programs that simulate the human thought-process, takes over. For example, at the center of Nasdaq's Sonar system, up to 18,500 newswire stories, 1,000 quarterly/annual reports filed by companies with the SEC, and price/volume models for 25,000 securities traded on the Nasdaq, OTC and Nasdaq-Liffe futures markets are processed each day.

Meanwhile, the AMEX Market Surveillance Knowledge Automation System also provides databases showing stock price history for each traded company—along with a spreadsheet including menus and macros to isolate periods warranting investigation. The system then yields a series of questions, answers to which result in one of two scores, one suggesting an investigation, the other for dropping the matter.

So a stock tripling in volume from one day to the next, as Imclone did on Dec. 26-27, 2001, automatically gets the appropriate exchange's attention. The staff then determines whether the activity could have resulted from company or industry news, an analyst report, or some other reasonable and public explanation. If no reason can be determined, the brokerage firms handling either side of transaction are asked for details about the trades and customers involved. Databases containing public information identify links between investors and possible information sources from within the company. Interviews of brokers, investors and company employees follow, to uncover improper relationships. If suspicions play out—and the exchanges stress that neither company nor transaction size matter—the exchange alerts the SEC, the other exchanges, and the Securities Investor Protection Corp. to jointly develop evidence for a civil case. In some instances, the Department of Justice or State Attorney's office may become involved, as we are now seeing in criminal cases.

Companies can help their executives, employees and vendors avoid getting snared. A written, regularly updated policy statement is a good beginning. Other steps include advance approval for trades by personnel at sensitive levels, written acknowledgments from those with access to sensitive information—and periodic refresher courses for those who face the public frequently. As Ms. Stewart can attest, being caught in the glare is anything but "a good thing."

Mr. Kalt is a principal of Kalt, Rosen & Co., a San Francisco consulting firm.