WILMER, CUTLER & PICKERING

e-commerce news

May 31, 1999

Online Trading: Enforcement Developments

In the U.S., more than one-third of securities trades by individuals now take place online. In a coordinated series of high-profile administrative and civil proceedings and investigations, or "sweeps," the U.S. Securities and Exchange Commission ("SEC" or "Commission") has taken aim at a variety of securities-related activities on the Internet.

The SEC, as the agency chiefly responsible for the enforcement of the federal securities laws, has devoted a substantial amount of its resources to monitoring, investigating, and prosecuting Internet securities fraud.

As the Director of the SEC's Division of Enforcement recently observed, although the scams and schemes perpetrated through the Internet are not markedly different from those the Commission has been prosecuting for years, certain of the web's unique informational attributes — low cost, high speed, wide distribution, easy access, deceptively professional-looking media, and anonymity of authorship — render cyberspace a particularly fertile ground for the purveyors of securities fraud. Indeed, these same attributes — particularly the high speed of information flow — are presenting the Commission and other regulators with new regulatory challenges that may ultimately need to be addressed with new legislation.

Commitment of resources. In response to the growing problem of Internet securities fraud, the Commission created an Office of Internet Enforcement (OIE) within its Enforcement Division in July 1998. OIE coordinates and trains a "Cyberforce" of 125 Division of Enforcement employees who voluntarily concentrate on Internet fraud cases in addition to their other duties and assignments.

OIE and the Cyberforce have developed a practice of conducting "sweeps" with "swat teams" in which they identify a group of potential Internet securities laws violators, conduct fast-paced investigations with concentrated resources, and then bring a group of administrative enforcement or civil injunctive actions simultaneously. The first such sweep was announced in October 1998, when the Commission brought twenty-three administrative and civil injunctive actions against 44 people and companies, focused primarily on "touting" fraud. The second occurred in February 1999, naming additional touters, and a third occurred earlier this month, focusing primarily on fraudulent and fictitious stock offerings. Given reports that the SEC is currently investigating a number of day trading websites, it is likely that the next sweeps will be brought soon and may concentrate on market manipulation issues.

What is touting? "Touting" is the practice of providing favorable profiles, descriptions, or recommendations of companies offering publicly-traded stock aimed at increasing investor interest in the stock, in which the touter purports to be providing an objective, unbiased opinion, but actually has an undisclosed

financial motivation for providing the information. This financial motivation can be, among other things, compensation from the profiled companies in the form of cash or securities, or a position in the stock of the profiled company that the touter intends to liquidate after the tout is released to the public. Such touters may be found among otherwise legitimate investor relations firms, financial advisory firms, and newsletter publishers, many of who have discovered the Internet to be an excellent medium for the dissemination of their touts.

The SEC is particularly concerned with the touting of "microcap" issues or "penny stocks." This concern stems from the fact that such companies are thinly capitalized, their stocks are thinly traded, and there is little independent information about them available -- characteristics that render such issues particularly susceptible to fraud. Such touts appear in various Internet media, such as websites, company bulletin boards, unsolicited broadcast e-mails or "spam," and chat rooms.

The touter's failure to disclose that it is receiving or has received compensation from the companies it profiles can constitute a violation of Section 17(b) of the Securities Act of 1933 (the "'33 Act"). Most of the cases the Commission brought in its October 1998 sweep were based on violations of Section 17(b). In one such case brought by the SEC's Southeast Regional Office in Miami, Florida, the Commission accused Princeton Research of touting stocks of five small companies without disclosing that the company and its president had received a substantial amount of stock and stock options from those companies. The Commission has also cited touters for inadequate disclosures, disclosures that degrade over time, and disclosures that can only be accessed through a web page link.

What is scalping? "Scalping" is a practice related to touting in which the touter fails to disclose its own position in the stock and then sells the position after the tout is released to the public. The Commission views scalping as a deceptive practice under the federal securities laws because the touter's intention to sell its own holdings is information the potential investor should have before deciding on the degree to which he or she will rely on the information provided by the touter. A number of the touting cases brought in the October 1998 sweep included scalping claims in violation of the anti-fraud provisions of the '33 Act and the Securities Exchange Act of 1934 (the "'34 Act"). In one such case involving a website called Stockstowatch.com, the SEC charged that the company that operated the website and its president made a profit of more than $1 million by selling the stocks of a least five small companies at the same time they were touting them on the Internet. The SEC alleged in its complaint that the website's failure to disclose the sales constituted a fraudulent device under Section 17(a) of the '33 Act and Section 10(b) of the '34 Act.

Touters can also run afoul of the federal securities laws for making false and misleading statements about the companies they profile and for paying cash or other incentives to brokers in an effort to convince the brokers' customers to purchase stock in the touter's profiled companies.

Fraudulent and fictitious offerings are frequent. Scam artists have made widespread use of the Internet to sell securities in companies or ventures that do not exist. Defrauders also make false and misleading statements about the prospects, capabilities, or earnings of the companies whose stocks they are profiling. The Internet has also been repeatedly used for the sales of unregistered securities. Regulators have reported illegal sales over the Internet in the stocks of offshore gambling enterprises, time travel technology, Hollywood movie theme restaurants, air-conditioning companies, and helicopter production companies, and in a fictitious debt instrument called a "prime bank note." The SEC has brought cases against individuals offering securities in a virtual casino website, an eel farm, and Costa Rican coconut plantations.

What is market manipulation? Market manipulation is the deliberate and artificial inflation of the market price of a security through the dissemination of false or misleading information about the issuer of that security. The greater the dissemination, the greater the potential effect the false or misleading information may have on the stock price. Given the breadth of dissemination achievable on the Internet, the Commission has reason to be concerned about market manipulation. Typically, these market manipulations take the form of "pump and dump" schemes, in which the holder of a substantial position in the security of a particular company spreads positive but materially false or misleading information about that company to drive up the market price of the security. The holder then sells the security for a large profit at the expense of other investors who fail to sell their own positions before the

holder's sale of his own large position causes a drop in the market price of the security from its artificially inflated level. Such false and misleading information can take the form of baseless price predictions, fictitious earnings or other positive fundamentals, and false or exaggerated claims about the company's products or prospects.

One new form of potential market manipulation unique to the Internet is currently receiving close scrutiny by the Commission. Day traders "chat up" a hot stock pick of the moment in chat room postings, begin trading in the stock, and (just as suddenly) announce that the stock price is falling and that everyone should sell his or her position in that stock. In the interim, the price of a particular stock may have risen and fallen dramatically. The chat room phenomenon raises a series of difficult questions: are the participants deliberately coordinating their buying activities to drive up the market price of the stock, or have other external market forces (such as positive news releases) also affected its price?

Apparently, the complexity of these questions has not prevented the Commission from probing the activities of such Internet sites. It may well be that the next Cyberforce sweep will involve cases in which the Commission tries to expand the definition of market manipulation to include the use of day trading websites and chat rooms.

Stay tuned. As use of the Internet continues to grow, there can be little doubt that the frequency of cyberspace securities fraud will only increase. It remains to be seen whether the Commission's high-profile Internet prosecutions will succeed in slowing this trend.

Monthly Update

Broad Internet legislation. Two pieces of broad Internet legislation were introduced jointly by Reps. Rick Boucher (D-VA) and Bob Goodlatte (R-VA). The first, H.R. 1685, the Internet Growth and Development Act of 1999, aims to provide for the recognition of electronic signatures for the conduct of interstate and foreign commerce, to restrict the transmission of certain electronic mail advertisements, to authorize the FTC to prescribe rules to protect the privacy of users of commercial Internet websites, and to promote the rapid deployment of broadband Internet service. The second, H.R. 1686, the Internet Freedom Act, eliminates FCC regulations on broadband development, declares ISPs and phone companies who prevent other carriers from entering the broadband market in violation of the Sherman Act, and prohibits the sending of unsolicited commercial email.

Privacy. Sen. John McCain (R-AZ) announced that he will hold a hearing this summer to examine the state of online privacy. According to McCain, the hearing will focus on whether consumers understand privacy policies and whether companies are following their posted policies. Sen. McCain's announcement followed release of a Georgetown University study finding that almost two-thirds of the web's busiest sites display some form of privacy policy.

Privacy/financial services. On May 4, President Clinton unveiled a privacy initiative, outlining ways to protect the privacy of consumers of financial services and to improve access to those services for lower income people. House Banking Committee Chairman Jim Leach (R-IA) spoke in favor of the initiative, urging greater disclosure of ATM fees and a bar against disclosure of personal medical information. On May 25, Rep. Jay Inslee (D-WA) introduced the Banking Privacy Act, legislation that would require that banks explain to customers how their data would be used and would give customers the right to "opt out" within 30 days. The Senate Banking Committee will hold a hearing on privacy, focusing on how the issue affects the financial services industry, on June 9, 1999 at 10:00 a.m.

Privacy/medical records. Another medical records privacy bill was introduced in the House this month. Rep. Gary Condit (D-CA) introduced H.R. 1941, the Health Information Privacy Act of 1999. The bill is based on three fundamental principles: (1) health information should not be used or disclosed without the authorization or knowledge of the individual, except in narrow circumstances where there is an overriding public interest; (2) individuals should have fundamental rights regarding their health records, such as the right to access, copy, and amend their records, and the opportunity to seek protection for especially sensitive information; (3) federal legislation should provide a "floor," not a "ceiling," so that states and the Secretary of Health and Human Services can establish additional protections as appropriate.

Database protection. The House Judiciary Committee approved legislation aimed at protecting electronic databases from copyright infringement (H.R. 354). The bill would create civil and criminal liability for anyone who extracts or uses in commerce all or a substantial part of a collection of information, causing harm to the market for that product or service. Although the legislation was reported favorably out of committee, there are still a number of concerns that need to be addressed before the bill goes to the floor. Rep. Howard Coble (R-NC) said the bill was still a "work in progress" and pledged to work with the Administration, Rep. Zoe Lofgren (R-CA), and others to iron out any differences.

More database protection. Rep. Tom Bliley (R-VA) introduced legislation to promote electronic commerce through improved access for consumers to electronic databases including securities market information databases. Like H.R. 354, H.R. 1858, the Consumer and Investor Access to Information Act, creates protection for databases but contains exclusions for news reporting and other functions. The bill also provides database publishers with protections against theft of their databases.

SPAM. Rep. Gene Green (D-TX) introduced the fourth piece of anti-spam legislation this year. H.R. 1910, the E-mail User Protection Act, attacks the problem of spam in a number of ways. First, the legislation makes it illegal to falsify any identifying information such as e-mail addresses or routing information. Second, the bill makes it illegal for a spammer to misappropriate or take over an unsuspecting person's e-mail account to spam others by subjecting the spammer to either a stiff financial penalty and/or possible jail time. Third, the legislation requires spammers, on the request of an individual, to remove them from their spam lists. Fourth, the bill makes it illegal to create, use, or distribute software that is primarily designed to falsify e-mail-identifying information. Finally, any violation of these provisions will lead to a fine of either $50 per violating message or up to $10,000 a day. Other pending anti-spam measures include: S. 759, H.R. 1685, and H.R. 1686.

For further information, contact:

David R. Johnson	djohnson@wilmer.com 202/663-6868
Susan P. Crawford	scrawford@wilmer.com 202/663-6479
Jeffrey E. McFadden	jmcfadden@wilmer.com 202/663-6385