STATE SECURITIES REGULATION AND THE INTERNET

*Marc S. Crandall**

INTRODUCTION

It was once said that any criminal who fails to exploit the Internet to promote a scam should be sued for malpractice. Indeed, with the popularity of the Internet, unscrupulous individuals have sought to take advantage of emerging technologies to defraud the public.[1] The Internet has become the marketing vehicle of choice for those committing securities violations. It is a global, borderless trading environment that offers instant access to millions of people. Criminals can maintain a certain amount of anonymity through the use of fictitious names and Internet cafés. Securities regulators struggle to adjust old legal constructs to a new medium. They must master a plethora of issues, including the application of existing laws to the Internet, the various forms of violations occurring online, investigative techniques, emerging technologies, and enforcement remedies. While state and local governments have defined jurisdictional boundaries, criminals can operate on the Internet from anywhere in the world.

California was one of the first states to recognize the threat to investors from unscrupulous dealers who are intent on defrauding consumers using the Internet.[2] The California Department of Corpora-

* Marc S. Crandall is an attorney for the California Department of Corporations. The views expressed by Mr. Crandall are his own and do not necessarily reflect the views of the California Corporations Commissioner or the policy of the California Department of Corporations.

1. *See* Press Release 98-11, Cal. Dep't of Corps., Internet Investments Ordered to Stop Selling (June 10, 1998) (on file with the *New York University Journal of Legislation and Public Policy*); Press Release 00-11, Cal. Dep't of Corps., Department of Corporations Files Internet Market Manipulation Actions (June 20, 2000), http://www.corp.ca.gov/pressrel/nr0011.htm (last visited Nov. 13, 2001) (on file with the *New York University Journal of Legislation and Public Policy*).

2. Cal. Dep't of Corps., *Fighting Internet "Cyber Investment Fraud," at* http://www.corp.ca.gov/pub/cyber.htm (last visited Nov. 13, 2001). The California Department of Corporations, originally named the State Corporations Department, was created in accordance with the Investment Companies Act of 1913. 1913 Cal. Stat. 715, ch. 353, § 16.

tions,[3] California's state investment and financing authority, licenses and regulates a variety of businesses, including securities brokers and dealers, investment advisers and financial planners, and certain fiduciaries and lenders. The Department also regulates the offer and sale of securities (investments), franchises, and off-exchange commodities.[4]

In 1998, the Department's enforcement division established the Internet Compliance and Enforcement Team (ICE Team) to address violations of laws involving the Internet and subject to the Department's jurisdiction.[5] The ICE Team administers a comprehensive program of legal analysis, surveillance, investigation, training, and prosecution. As part of its regulatory activities pertaining to the Internet, the Team seeks to discover unqualified and nonexempt securities offerings, fraud in connection with the offer or sale of securities, unlicensed investment advisor or stockbroker activity, and stock market manipulation. The goal of the Department is to create a safer online environment for legitimate businesses seeking to raise capital and for investors in these businesses.[6]

I
THE SECURITIES LAWS

The California Corporations Code requires that any individual or entity seeking to sell investments within the state obtain a permit for such offering from the California Corporations Commissioner.[7] Specifically, the Commissioner must determine that the offering is "fair, just, and equitable."[8] The justification for requiring qualification is quite straightforward. Without full disclosure of the financial and other information relating to an offering, and the application of the "fairness" standards to protect the public investor's interests, an investor would have little confidence in the true value of an investment.

---

3. To find out more about the California Department of Corporations, visit its Web site at http://www.corp.ca.gov.

4. *See* CAL. CORP. CODE §§ 25000–31516 (West 1977 & Supp. 2001).

5. Press Release 00-11, *supra* note 1; *Fighting Internet "Cyber Investments Fraud," supra* note 2; Gwendolyn Mariano, *Stock Fraud Spurs Regulators to Look Online*, CNET NEWS.COM (June 21, 2000), *at* http://news.cnet.com/news/01-1005-200-2126256.html (last visited Nov. 11, 2001) (on file with the *New York University Journal of Legislation and Public Policy*).

6. The information included in this article regarding the ICE Team is primarily based upon the author's experience working for the California Department of Corporations. For other information about the ICE Team, see Press Release 00-11, *supra* note 1; *Fighting Internet "Cyber Investments Fraud," supra* note 2.

7. CAL. CORP. CODE §§ 25111–25113 (West 1977 & Supp. 2001).

8. *Id.* § 25140(c).

By analogy, in the purchase of a second-hand automobile, it would be imprudent for a consumer to complete a transaction based solely on the representations of the seller. Instead, a cautious consumer will scrutinize the automobile, kick the tires, and take it for a test drive. Unlike the above scenario, there is no tangible product available for review in a securities transaction. Furthermore, the purchase of a security is especially perilous because individuals often invest substantial sums of money. Thus, it is crucial that an investor's purchasing decision be based on reliable information provided by the offeror. Without access to this information, an investor would be forced to rely solely on the offeror's representations.

Accordingly, United States federal and state securities regulators require companies to register or qualify their securities offerings.[9] In addition, issuers must disclose, on a regular basis, financial and other information about the company.[10] During the registration or qualification process, the information is reviewed before it is made available to the public. The disclosure allows members of the public to "look under the hood" of the offering company, in order to make an informed, independent evaluation of the company and the value of the securities.

Note that not all securities offerings require qualification or registration. Exemptions to the process do exist, especially if the offeror does not plan to sell investments to the general public. For example, some entities intend only to offer securities to friends, family, business colleagues, or to those who can bear the financial risk and have substantial investment experience or expertise. Accordingly, state and federal law provide for exemptions to the qualification or registration requirements, based, for example, upon a prior relationship or the business sophistication of the investor.[11]

II
ILLEGAL OFFERINGS

Many individuals have utilized the Internet in ways that run awry of the securities laws. For example, even some transaction exemptions do not permit the public solicitation of investors.[12] However,

9. *See* Securities Act of 1933 § 5, 15 U.S.C. § 77e(c) (1994); CAL. CORP. CODE §§ 25111–25113.

10. *See* Securities Exchange Act of 1934 § 12, 15 U.S.C. § 78l (1994 & Supp. 2000); CAL. CORP. CODE § 25146.

11. *See* Securities Act of 1933 §§ 3–4, 15 U.S.C. §§ 77c–d (providing exemptions of certain classes of securities transactions); Regulation D, 17 C.F.R. §§ 230.501–506 (2001); *see also* CAL. CORP. CODE §§ 25101–25105.

12. CAL. CORP. CODE § 25102(f).

individuals have often posted such solicitations on Web sites used to promote their businesses. In many of the cases investigated by the Department, much of the information on the Internet offerings was inherently misleading. Risks were downplayed and results were guaranteed. Issuers failed to qualify the offerings with the Department of Corporations or to comply with the terms of available exemptions and failed to disclose this fact on their Web sites.[13]

Some enforcement actions involve rather imaginative offerings. An early administrative action, brought in 1998, concerned a United Kingdom-based Web site offering bonds to the public to develop a time machine. The author claimed that the investment opportunity could not lose. Even if the company itself could not construct a time machine, the research would generate so much publicity that someone in the future would come back in time and show the company how to develop the appropriate technology.[14]

Of course, such far-fetched offerings, though amusing, are not as dangerous to investors as those that appear plausible. Some Web sites fool investors quite effectively. In one of the first criminal actions involving Internet violations of the securities laws, a California individual sold investments in a company to develop an Internet telephony device. The individual collected more than one hundred thousand dollars and used the funds for personal gain. The individual was ultimately sentenced to ten years in prison.[15]

III
MARKET MANIPULATION AND TOUTING

Information disseminated online can have a substantial effect on the securities markets, and unscrupulous individuals have taken advantage of the Internet for their financial gain. While stock market manipulation is quite different from the fraudulent sale of securities, both activities violate federal and state securities laws.[16] A common

13. *See* Press Release 99-12, Cal. Dep't of Corps., State Internet Sweep Nets "Illegal and Fraudulent" Entertainment Investments (July 28, 1999) (on file with the *New York University Journal of Legislation and Public Policy*).

14. *See* Press Release 98-11, *supra* note 1.

15. *See* Sucheta Dalal, Desi *Regulations for Local Conditions*, REDIFF.COM, Feb. 14, 2000, *at* http://www.rediff.com/money/2000/feb/14dalal.htm (on file with the *New York University Journal of Legislation and Public Policy*); Reuters, *Man Arrested on Net Stock Fraud Charges* (Apr. 9, 1998), http://www.wired.com/news/business/0,1367,11575,00.html (on file with the *New York University Journal of Legislation and Public Policy*).

16. Securities and Exchange Act of 1934 § 10, 15 U.S.C. § 78j (1994); CAL. CORP. CODE §§ 25400–25401.

ploy involves the purchase of securities at a low price. The perpetrator then posts fraudulent messages on bulletin boards promoting the securities. To generate additional excitement and trading momentum, a perpetrator may create multiple identities and post messages as several different individuals. The messages create an illusion of trading activity. If enough people are fooled, actual trading activity may develop, driving the price to artificially inflated levels. Once the trading price reaches these levels, the perpetrator will sell his or her shares at an incredible profit.

One example of such a case involved Pairgain, a technology company headquartered in California. The perpetrator posted a message on a Yahoo! bulletin board indicating that Pairgain was to be purchased by an Israeli company. The perpetrator included a link to an alleged Bloomberg Web site containing a news article that described the sale. The price of the security was affected within hours. However, the Web site and news article embodied therein were fabricated by a Pairgain employee.[17]

Another case involved an individual posting messages on a Yahoo! bulletin board posing as Metro Goldwyn Mayer's (MGM's) former chairman. The messages alluded to MGM stock pricing predictions allegedly made by MGM's majority stockholder. MGM and the individuals allegedly involved denied any involvement with the messages. Eventually, the ICE Team identified the subject and learned that he had been actively trading MGM securities at the time he posted the messages. The Department of Corporations initiated a regulatory action against the individual.[18]

On occasion, securities law violators utilize more creative means to disseminate fraudulent information. In the case of Emulex, a technology company's securities were manipulated by an individual who issued a false press release. The false press release was eventually carried by several well-known news organizations. The wide dissemination of this information had a disastrous effect on the price of the Emulex stock.[19]

Some companies, unhappy with the performance of their own stock, hire others to promote the company's securities. In exchange

17. *See* Jonathan Gaw, *Internet Hoax Sends O.C. Tech Stock Up 31%*, L.A. TIMES, Apr. 8, 1999, at A1.

18. *See* John Geralds, *US Agency Settles Alleged Online Stock Scam*, VNUNET (June 23, 2000), *at* http://www.vnunet.com/news/1104471 (on file with the *New York University Journal of Legislation and Public Policy*); Mariano, *supra* note 5.

19. *See* Peter Y. Hong, *Man Pleads Guilty in Stock Hoax*, L.A. TIMES, Dec. 30, 2000, at B5.

for these services, companies will occasionally compensate promoters with shares of stock. Thus, if the company is promoted effectively, promoters earn money as a result of the increased stock value. Promoters often choose to distribute mass e-mails to promote the stock, posing as investment advisers or financial analysts. However, promoters who fail to disclose to the public the receipt of compensation in connection with promotional activities invite regulatory action.[20] Selling into their own buy recommendation without disclosing the conflict raises serious issues of fraud.

IV
UNDERCOVER OPERATIONS AND SURVEILLANCE ACTIVITIES

The Department obtains leads from a number of sources: surveillance, undercover operations, junk e-mail, public complaints, and referrals from other law enforcement agencies. It is advantageous for regulators to assume a low profile, especially when investigating a suspect. Unfortunately, the architecture of the Internet does not normally permit the anonymity required for undercover operations. A technically savvy suspect could design a Web site that would reject access to computers linked to government networks, or reroute access to a Web site that complies with the law. Thus, ICE Team members avoid conducting surveillance activities from state computer terminals. The ICE Team utilizes public Internet service provider accounts when accessing the Internet. When the ICE Team conducts investigations in such a manner, a suspect cannot normally differentiate between a casual Internet user and an ICE Team investigator. ICE Team members also utilize free Web-based e-mail accounts when actively engaging a suspect. Indeed, it is unlikely that a suspect will respond to an investigator's inquiry if the investigator's e-mail address ends with ".gov".[21]

The ICE Team also utilizes search engines during surveillance activities. Popular search terms might include "investment opportunity," "get rich quick," "easy money," "inside information," or "guaranteed profit." However, the use of search engines to generate cases is not necessarily an effective use of resources. Generic Web-based search engines or "Web crawlers" review thousands of Web sites and catalog the text embodied therein in massive databases. When an in-

20. *See SEC Files Four Fraud Actions Against Internet Stock Promoters*, SEC. & COMMODITIES LITIG. REP., Mar. 24, 1999, LEXIS, Secltr File.

21. *See Fighting Internet "Cyber Investments Fraud," supra* note 2; discussion *supra* note 6.

dividual conducts a search, the search engine compares that inquiry with text cataloged in the engine's database. If a match exists, the search engine displays the corresponding Web address, allowing the user to click on the address and review the Web site. However, the Web sites containing that text might have been cataloged by the search engine years earlier. Web-site content is dynamic—a Web-site operator may change content information many times a day or remove the site entirely. Thus, search results may be outdated or too voluminous to be of use for enforcement purposes.[22]

Accordingly, some Internet surveillance units choose to monitor areas of the Internet that attract active illegal solicitations, such as Web-based bulletin boards, chat rooms, and Usenet newsgroups. Indeed, both seasoned and novice investors look to these services as a source of investment information. A criminal can easily target potential investors by posting messages to such sites. It is therefore more effective for regulators to monitor bulletin boards and chat rooms for illegal activity than to conduct Web searches.

Still, search engines do play a vital role in providing information once a target has been identified. In fact, in one investigation, the Department received a written complaint about a company selling unlicensed investments through Internet mass-mailings and telemarketing centers. At the time, the Department was aware of only three investors. Once the ICE Team researched the suspect company's name online, the ICE Team identified more than a thousand additional victims.[23]

Unsolicited e-mail also results in regulatory actions. It is most often used to sell unqualified and nonexempt securities, or to manipulate the price of legally traded securities. To obtain access to these messages expeditiously, the ICE Team members post undercover e-mail addresses on bulletin boards and newsgroups. Occasionally, bulk e-mail providers will collect these e-mail addresses and incorporate them into massive electronic mailing lists. Eventually, the ICE Team begins receiving e-mail solicitations, often permitting the Department to take action before substantial damage to investors can occur.

Once illegal activity has been documented, the ICE Team must identify the suspect. The ICE Team utilizes different techniques based on a case's unique circumstances. For example, if an individual posts

22. *See* Danny Sullivan, *How Search Engines Work*, SEARCH ENGINE WATCH, *at* http://www.searchenginewatch.com/webmasters/work.html (last updated June 26, 2001) (on file with the *New York University Journal of Legislation and Public Policy*).

23. This case is still under investigation and, as such, the details are confidential.

fraudulent messages on Web-based bulletin boards, the appropriate Web-site operator will be contacted to determine whether identifying information can be obtained. In most cases, the ICE Team can trace this information to the suspect's Internet service provider until the suspect is identified. When researching a particular Web site, ICE Team members identify which Internet service provider maintains the site for the suspect. Information surrounding the registration of the Web site's domain name address is also researched and catalogued.[24]

The Department has at its disposal a number of legal remedies to address violations of the state's securities laws. The Commissioner may issue administrative orders to halt violations of the laws; to deny, censure, suspend, revoke, or take possession of licensees; and to censure, suspend, or bar individuals from participating in an industry.[25] The Department may also bring civil injunctive actions in the name of the people of the State of California to enjoin violations of the laws, to appoint receivers over companies, and to obtain equitable remedies including rescission, restitution, and penalties against the violators.[26] Finally, the Department may refer violations of laws to the appropriate agency for criminal prosecutions, as well as participate in the investigation and prosecution of the violators.[27] Since the Department's first Internet securities enforcement sweep, the ICE Team has assisted in enforcement actions against hundreds of companies and individuals engaged in the illegal and fraudulent offering of investments and financial services, unlicensed investment adviser and broker dealer activity, and market manipulation.[28]

CONCLUSION

The Internet offers a number of advantages to criminals. It provides inexpensive access to millions of potential victims. The criminal enjoys a certain amount of anonymity while presumably achieving credibility derived from an Internet presence. However, the Internet also offers criminals a number of disadvantages. Internet solicitations increase the risk of detection by any law enforcement agency with Internet access. Furthermore, once a fraud has manifested itself, the public can post information or warnings on Internet bulletin boards or in chat rooms. Finally, utilizing the Internet to promote a scam, espe-

24. See The Internet Corporation for Assigned Names and Numbers at http://www.icann.org for more information about the domain name registration system.
25. CAL. CORP. CODE §§ 25530–25534 (West 1977 & Supp. 2001).
26. *Id.* § 25535.
27. *Id.* § 25533.
28. *See Fighting Internet "Cyber Investment Fraud," supra* note 2.

cially in the form of bulk e-mail solicitations, may expose the criminal to civil and criminal liability in multiple jurisdictions.

The public should exercise caution when using the Internet in connection with investment activities. It is unwise to make a buy or sell decision based solely on what is read online, or on anonymous "stock tips." In addition, Web sites that lack contact information should be avoided—especially those sites promising high returns and low risk. Investors should not hesitate to contact their securities regulator with any concerns.[29] Finally, investors should always remember that if something looks too good to be true, it probably is.

29. To contact the United States Securities and Exchange Commission, go to its Web site at http://www.sec.gov. To locate a state or provincial securities regulator, visit the North American Securities Administrators Association's Web site, at http://www.nasaa.org. To identify a securities regulator in a particular country, visit the International Organization of Securities Commissions at http://www.iosco.org.