INSIGHTS

THE CORPORATE & SECURITIES LAW ADVISOR

Volume 12, Number 2, February 1998

Year 2000: Disclosing the Risks to Markets and Firms

Page 4

VIVIAN A. MAESE of Salomon Smith Barney Holdings, Inc. and MICHAEL D. MANN and DONNA I. DENNIS of Richards Spears Kibbe & Orbe discuss the Year 2000 problem and offer suggestions to assist corporate counsel and other concerned parties in identifying and reducing the substantial business, regulatory, and litigation risks that it poses.

The Internet's Impact upon SEC Rules Of Engagement

Page 10

JOHN REED STARK of the SEC Division of Enforcement explores how the Internet has transformed the SEC enforcement program, not only changing what it enforces, but also how it does so.

Executive Compensation Practices May Limit Change of Control Severance Benefits

Page 15

MICHAEL KATZKE of Wachtell, Lipton, Rosen & Katz examines the impact that executive compensation arrangements may have on the ability of employees to receive full severance benefits following a change in control.

DEPARTMENTS

SECURITIES ENFORCEMENT

Tombstones: The Internet's Impact Upon SEC Rules of Engagement

The SEC enforcement program has always evolved to address the ever-changing dynamics of domestic and global financial markets, and leaving a few tombstones behind is really nothing new. Yet, the enforcement division has never before experienced such a rapid and extreme transformation as the one initiated by the Internet. This article discusses five illustrations of how the Internet has transfigured SEC enforcement's rules of engagement, not only changing what to enforce but also changing how to enforce.

By John Reed Stark

Here Lies Lester Moore, Shot 4 Times With a 44, No Les, No More.

Interment is never an easy subject to discuss and does not typically fall within the jurisdiction of the Division of Enforcement of the United States Securities and Exchange Commission (SEC). But with the onslaught of the Internet, old concepts and notions of the traditional SEC enforcement paradigm continue to sound their own death knell, leaving only tombstones to mark their passage. As the Internet chisels the epitaphs on these tombstones, newborn principles and postulates infuse themselves into the SEC enforcement program.

John Reed Stark is special counsel for Internet Projects in the Division of Enforcement of the United States Securities and Exchange Commission (SEC) and is in charge of the Division's Internet Program. He is also an adjunct professor of law at Georgetown University Law Center where he teaches a course on the Internet and the Securities Laws. The SEC as a matter of policy disclaims any responsibility for any private publication or speech by any of its members or staff. The views expressed herein are those of the author and do not necessarily reflect the views of the SEC or the author's colleagues on the staff of the SEC. All quotes in the section headings of this article, including the Epitaph (found at Boot Graveyard in Tombstone, Ariz.), are from the film *Tombstone* (Hollywood Pictures Corporation, 1993), produced by James Jacks, Sean Daniel and Bob Misiorowski, directed by George Cosmatos and starring Val Kilmer and Kurt Russell as the famed Doc Holiday and Wyatt Earp.

The five illustrations that follow demonstrate that the Internet continues to change the playing field, requiring the SEC enforcement division to modify its *modus operandi* and flex its regulatory muscle, to combat this nascent and potentially dangerous threat to investors.[1]

I'm your Huckleberry and that's just my game.

The New Cyber Boiler-Rooms

Consider the fictional owner of an imaginary company called PhenomX, a manufacturer of a purported cure for cancer. To date, PhenomX has not sold any products, has not hired any employees, has not generated any income from operations, has only nominal assets, and has just begun to be quoted on the OTC Bulletin Board. PhenomX has just submitted its application for FDA approval of its sole drug, which PhenomX's president knows the FDA will reject; he knows this because the drug is merely coffee grinds in tablet form.

PhenomX's president, his family members and a few friends own all the ten million shares outstanding. The president, a recidivist scam artist, wants to pump up the price of PhenomX fraudulently, and sell his shares at the artificially inflated price. The president has only limited resources to set up a boiler room or to fund any other network of fraudsters; all he has is a little capital, a home computer, some Internet-related software, and Internet access. Unfortunately, that is all he needs. At almost no cost, the president can conduct an international and sophisticated market manipulation over the Internet from his own living room. All PhenomX's president must do is to take the four following steps:

Step 1: The Phony Web Page

The first step for PhenomX's president is to set up a central location on the Internet where potential investors can find out about PhenomX's miracle drug, in an interactive and user-friendly environment. On the World Wide Web space allocated to him for free by his Internet access provider, the president builds a flashy and elaborate PhenomX Home page.

The page presents a wide range of bogus enthusiastic reports about PhenomX, including a phony set of

financial statements inflating the value of the potential PhenomX drug's patent and documents bearing the FDA seal with the actual names of FDA staff members asserting imminent FDA approval for the PhenomX drug. Despite the president's lack of experience with computer programming, he easily constructs the page with a simple Web page development software package downloaded free of charge from the Internet.

The page incorporates graphics, sound and video, all obtained for free from the Internet. The page even features a direct "video stream" that allows users to watch live action of PhenomX scientists hard at work (the video is a phony though users cannot tell the difference). In addition, the page contains all the information necessary for the purchase of PhenomX shares, a chat area for "real-time" talk about PhenomX, and a bulletin board allowing users to post messages.

Step 2: Spam, Spam, and Spam

The second step is to use email, via a bulk-email or a spamming[2] program, to contact as many potential investors as possible, about the fantastic investment opportunity that PhenomX represents. The PhenomX president employs a "mining" or "extractor" program that automatically collects email addresses from all over the Internet. He also spends some time personally gathering email addresses from the investment-related bulletin board systems, cyber message areas, newsgroups and the various Web discussion forums dedicated to speculative investing and unlisted securities. The president is relentless in developing an extensive email list of potential victims.

The president even collects a list of over 50,000 email addresses from sites dedicated to discussing Comparator Systems Corp. and Systems of Excellence, two of the most notorious stock manipulations involving the Internet—both companies the subjects of tens of thousands of Internet postings feverishly hyping their respective stocks.[3] The president reasons that if these people bought shares of Comparator and Systems of Excellence, they might purchase shares of PhenomX.

The president drafts a personalized note to explain that PhenomX represents an exceptional buying opportunity and is poised to skyrocket in price. On the note is a hyper-link to the PhenomX Web Site and a hyper-link to the page with all the necessary purchasing information. Next, with the click of a mouse, the president beams his personalized note to his private list of hundreds of thousands (even millions) of potential victims.

For still greater distribution, the president hires a bulk emailer, an entity that contracts to do mass mailings for a fee (typically about $100 per month) to send the email to several million more potential victims. Cybermailers boast that for every hundred emails sent out, seven responses result. This massive global solicitation is no longer a matter of opening up the white pages of the phone book and dialing every number— this is a customized mailing list of potential victims never before available to the average con artist.

Step 3: Begin the Buzz

Now PhenomX's president needs to create a "buzz" on the Internet about PhenomX. The president utilizes several means to accomplish this goal. The president smothers Internet forums with his spam (or some other marketing materials), by posting it to newsgroups and Web discussion areas dedicated to investing.

The president also creates discussion forums dedicated to talking about PhenomX while also posting his spam to discussion forums pertaining to other speculative securities, the whole time hoping to snare a few victims into purchasing PhenomX stock. The president responds to his own postings under various user names to create the illusion that people are having a discussion, when in reality it is just the president posting back and forth to himself, spreading more false information about "PhenomX."

Step 4: Tout or Bribe a Touter

The fourth and final step makes the buzz more sophisticated by employing an Internet investment newsletter. There are two options: the PhenomX president may personally construct his own Internet investment newsletter to recommend PhenomX, or, instead, bribe an unscrupulous online investment newsletter to feature PhenomX as the "pick of the month" or some other sham promotion.

To build a personal online investment newsletter, he simply chooses a catchy name, uses the same Web page building software employed for the PhenomX Web site, and beams the newsletter out (or a spam with a link to the newsletter) to the same list used for the PhenomX spam. The president posts the Internet address of the investment newsletter in various investment newsgroups and other online discussion forums that relate to investing. The newsletter, provided free of charge, even picks a few recent winners in the market and boasts that these stocks were prior newsletter picks.[4]

There it is–four easy steps to a successful "pump and dump" scheme, courtesy of the Internet. Don't doubt this four-step scenario. Record numbers of individuals

own securities, and expect to receive double (and times triple) digit returns on stock investments. Hordes of neophyte investors have jumped head first into the stock market, experienced the boom of the past few years, and are hungry for more. This phenomenon exacerbates susceptibility to online fraud schemes like the one promulgated by the fictional PhenomX company, and marks this new crop of investors as potential targets for investment fraud.

Are you gonna do something or just stand there and bleed?

The New Offshore Cyber Fraud

There was a time when the offshore orchestration of a fraud upon U.S. investors, unless targeted towards the wealthy, was almost cost-prohibitive. Consider the operation of an offshore boiler-room selling a fraudulent investment opportunity. A boiler-room depends on two important elements for its success: first, the ability to contact a large number of potential investors and, second, the wherewithal to make the sale to the potential victim before the victim has time to deliberate about the investment. Conflicting time zones, differing currencies and most of all, the sheer costs of long distance telephone calls, overnight mailings and other communication-related expenses all contribute to hindering offshore fraudsters from preying on U.S. individual investors.

The Internet has, of course, changed all this. With the rapidly diminishing costs of Internet access, computer hardware and Internet-related software, a fraud emanating from the most remote emerging capital market costs about the same as one that emanates from the house next door, perhaps even less. International con artists can use Web pages, email, newsgroups, discussion forums and chatrooms just as easily as anyone within the United States. The obstacles created by differing time zones and other traditional notions of borders disappear when it comes to the Internet, and soon, universal digital legal tender may even reduce the problems caused by different currencies.

Internet offshore fraud may become the single greatest threat to U.S. investors. It raises a myriad of complex issues and forces U.S. law enforcement to rethink traditional notions of jurisdiction and sovereignty. When considering an Internet fraud that involves a foreign jurisdiction, the enforcement division must address issues associated with investigating and prosecuting foreign entities and individuals, from serving subpoenas and criminal duality to locating assets and extradition.

What an ugly thing to say.

The New Cyber-Defamation (of Character and Corporation)

Spurious rumor-mongering has always pervaded Wall Street, whether done for the purposes of market manipulation or just for spite. Historically though, the rumor mongers were usually limited in the numbers of individuals they could reach. Now, with the availability of the Internet, spreading negative publicity about a company or an individual has never been easier. Instantaneously, efficiently, and at very little cost, individuals can use the Internet to cast dispersions upon the most reputable of companies and individuals, reaching millions.

The Internet has become saturated with negative deceptive information about companies and their employees. The nefarious short-seller uses the Internet to spread false information pertaining to a publicly traded company and the treacherous promoter uses the Internet to advance false scuttlebutt about competitors. Of course, many of these rumors and ramblings published on the Internet strain credulity, and are simply ignored by users, but the accuracy of some information is more difficult to discern, even when employing the highest level of skepticism.

No subject is sacred, even SEC activities. In some Internet discussion forums, for example, users gossip about an SEC investigation when no such investigation exists. Hopefully, most individuals do not believe a false rumor about an SEC investigation in such instances, particularly when the company or individual loudly and flatly denies the existence of the investigation.

But what if the company or individual cannot make such a representation – because, in fact, an investigation does exist. While pending, members of the public inevitably learn some information pertaining to an SEC investigation, typically from witnesses asked (or subpoenaed) to testify or produce documents pursuant to that investigation.[5] Although an SEC investigation is not meant to be an indication by the Commission or its staff that any violations of law have occurred, or a reflection upon any person, entity or security, public dissemination about an SEC investigation can still damage the reputation of an individual and a company (even impacting the company's stock price). This is one of the many reasons why the enforcement division maintains a long-standing policy of confidentiality and deems nonpublic even the mere existence of an investigation.

Before the Internet, witnesses seeking to propagate information about an existing investigation were limited in the means used for dissemination—they could

meet by the water-cooler, telephone, or use the mail to inform colleagues and friends. Now, with the increasing ease of Internet use, individuals can publish SEC correspondence and subpoenas, transcripts of testimonial proceedings, even information about SEC staff, such as the staff's background or possibly a home phone number. This could lead to even greater dangers. For example, a corrupt short-seller might learn of an actual SEC investigation from an Internet user, and then exploit the information, spreading a lie across the Internet that SEC is about to file a civil enforcement action, when the SEC staff are actually about to close the investigation.

You look like somebody just walked over your grave.

The New Cyber-Sleuths

Complaints and tips from members of the public have historically provided the largest single source of investigative leads for the enforcement division. Thus, it was only natural for the SEC to open its Enforcement Complaint Center (ECC) *(www.sec.gov/enforce/comctr.htm)* and expand the ways members of the public can contact the enforcement division to report potential securities violations over the Internet (or any other potential violation of the federal securities laws).

There is a genuine culture of vigilance and self-policing among Internet users, and the enforcement division hoped to tap into that culture and further its mission of protecting investors with the online construction of the ECC. The ECC, which began operation on June 14, 1996, provides a variety of means to contact the enforcement division, including an email box, toll-free number, fax number, and mailing address. The ECC also provides a user-friendly form to ensure that the complainant sends a complete report of the suspicious activity.

Thus far, returns from complaints made to the ECC have exceeded expectations. From its inception, the ECC began receiving about 100 complaints a week, and now receives more than 100 complaints each day. Not only does the ECC generate leads about specific entities and persons, but the ECC also permits the enforcement division to remain apprised of the latest trends and tactics of online riffraff.

Most startling is that complaints from Internet users are of a novel variety never encountered before. Hence, the genesis of the "Cybersleuth." The Cybersleuth reports more than just the fraudulent Web page or other potential Internet securities violation. Cybersleuths meticulously trace the headers of suspicious spams, relentlessly seeking to pierce any cloak of anonymity. Cybersleuths take time to provide painstaking details of potential violations, usually offering identifying information about themselves in case the SEC needs to contact them. Cybersleuths even list the potential securities violations of fraudsters by statute, rule and regulation, sometimes by precise citation. Cybersleuths receive no reward or bounty for their benevolence, just the satisfaction of helping to keep the Internet clean and safe for all investors, and their numbers continue to swell.

I am afraid we must redefine the nature of our association.

The New Cyber-Investigation of the Internet 'Killer Application'

A "killer application" is generally defined as any product that overwhelms the competition, significantly transforming a business - the first word processing package was a killer application as was Lotus 1-2-3. Not a day passes without business headlines announcing another company's progress in the hunt for the Internet's next killer application. The word is out—no arena is riper for the next killer application than securities, investments and finance. The enforcement division faces challenges on two fronts in this regard.

First, there are fraudsters who try to capitalize on the hype surrounding technology, feigning discovery of the next killer application and then operating a "pump and dump" scheme for their company's publicly traded stock.[6] Second, there are those who will implement new technologies like online trading facilities and Internet bulletin boards and unlawfully circumvent critical customer protection provisions embedded into the federal securities laws.

No matter what the fate of these futuristic market appliances, the bottom-line is that the enforcement division can no longer rely solely on its traditional investigative methods and tools of yesteryear to police the next killer application. The enforcement division now, more than ever, continuously updates its own computer and Internet resources while also engaging in proactive measures to take advantage of the Internet (and Internet killer applications) for its own benefit.

The enforcement division, for example, in the Internet's discussion forums, not only routinely announces SEC proceedings, such as trading suspensions,[7] but also collects information from members of the pub-

...[8] On the Web, the Enforcement Complaint Center ...scussed above provides an interactive area for inves...ors to communicate with the enforcement division directly.

The enforcement division also is constantly beefing up its technological arsenal, maintaining all the necessary online commercial provider accounts, T1 lines[9] for direct Internet access, and also employing the latest browsing software for viewing the Internet together with the powerful hardware necessary to do the job right.

So run you cur, and tell all the other curs the law's coming . . . you tell 'em I'm coming and Hell's coming with me you hear, Hell's coming with me.

Conclusion

As the rapid pace of technology continues to impact the SEC enforcement division, the newly fashioned ...yber transgressions of today could very well shape the ...pitaphs on the tombstones of the next millennium. Yet, one group of judicial precepts will always remain notably absent from the list of tombstones—the powerful antifraud provisions of the federal securities laws that have served the SEC so well since their inception. Historically, the flexibility of the antifraud provisions has provided a statutory basis for the enforcement division to prosecute offenses ranging from unlawful insider trading to fraud in the sale of derivatives to pay-to-play municipal bond schemes. Internet related securities violations do not require any new enforcement statutes, rules or regulations; the present range of antifraud provisions embodied in the federal securities laws more than suffice.

The Internet has created fantastic opportunities for companies, entrepreneurs, brokers, dealers, exchanges, and every other participant in the financial markets, and, in many respects, the investor has emerged as the biggest winner of them all. Investors now have instantaneous financial information of almost every variety at their fingertips—all at little cost, at any time and from the comfort and privacy of their own homes. Advanced concepts of electronic disintermediation and cyber-commerce will undoubtedly lead to better access, cheaper ...osts and fairer markets for all participants. The inves...or of today, with the help of the Internet, has become more informed than ever before.

Unfortunately, the Internet has also spawned a new generation of scam artist—a generation that aims to spoil the information superhighway, and contaminate the exciting new financial emporium the Internet has created. These miscreants believe that the Internet's uncharted territory provides the ultimate opportunity to modify the investment playing field in their favor. These folks are dead wrong.

Over the past 65 years, no matter where the arena, cyberspace or otherwise, the SEC and its enforcement program has remained committed to stamping out fraud and maintaining fair markets for all investors. In carrying out its mission, the enforcement program has left a graveyard of tombstones behind, continually adapting and modifying its own rules of engagement whenever necessary. The Internet merely accelerates the changes, because the tombstones no longer creep up casually, they shoot up, right under your feet.

NOTES

1. For a thorough discussion of the SEC's response to Internet fraud and other Internet-related threats to investors, and an overview of the SEC enforcement division's Internet Program *see*, Joseph J. Cella III and John Reed Stark, SEC Enforcement and the Internet: Meeting the Challenge of the Next Millennium A Program for the Eagle and the Internet, 52 Bus. Law. 815 (May, 1997).

2. Spammers, who practice their art by transmitting an email message to email lists (much like the junk mailer sends brochures, offerings and other information via U.S. mail), combines the skills of a mass mailer with the hard core pressure sales tactics of "boiler-room" cold-callers. Internet lore has it that the term "spam" derives from a famous Monty Python skit, which featured the word spam repeated over and over. The term may also have come from someone's derision of the eponymous generic processed meat product, which some perceive as lacking in substance or content. (Spam is a registered trademark of Hormel Corporation.)

3. *See, SEC v. Charles O. Huttoe, et al.*, Civil Action No. 96-CV-02543 (GK) (D.D.C.); SEC Litigation Rel. 15153 (November 7, 1996) and *SEC v. Comparator Systems, et al.*, Civil Action No. 96-3856 (JGx) (C.D. Cal.); SEC Litigation Rel. No. 15056, 1996 SEC LEXIS 2478 (September 19, 1996). 96-3856 (LGB)

4. Section 17(b) of the Securities Act of 1933, often referred to as an anti-touting statute, clearly prohibits an Internet user from posting certain promotional information and opinions concerning a security in an investment newsletter without also disclosing the nature and substance of any consideration received from the issuer of the company underlying that security.

5. When SEC enforcement staff contact a witness during an investigation, enforcement staff must provide certain limited information to the witness, such as the staff's principal purpose in requesting information from the witness, the name of the investigation and, of course, the identity of the investigating SEC enforcement staff. *See* The Privacy Act of 1974, 5 U.S.C. §552a (providing certain notice and protections to persons from whom the government solicits information).

6. *See* note 4, *supra.*

7. *See e.g.*, SEC postings on America online and on the Silicon Investor announcing the trading suspension of Rocky Mountain International at *http://www.techstocks.com/~wsapi/investor/reply?s=suspension+rocky+mountain&sreply=3021750.*

8. *See e.g.*, SEC postings on *The Silicon Investor* at *http://www.techstocks.com* seeking information concerning SGA GoldStar prior publications.

9. T1 lines grant access at 1500 bits per second (more than 50 times faster than the average high speed modem which only transfers 28.8 bits per second).