NSCP CURRENTS

A Publication of the NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

INFORMATION EXCHANGE

In the following consultations, the member was informed that the preliminary advice provided was subject to the accuracy and completeness of the facts recited, including the presence or absence, and the identities, of adverse parties. No attempt was made to investigate the facts represented to us. Any deviations from, or additions to, the facts as described to NSCP staff members could have warranted different conclusions and resulted in different advice.*

Insider Trading Safe Harbor

Q: A client of the firm is an officer of a public company, XYZ Corp. He wants to sell some of his holdings of XYZ at a time when one would expect that quarterly earnings are ready to be announced. He claims that his sales will not violate the insider trading provisions of the federal securities laws because his sales would take place pursuant to a prearranged plan. Can such plans really avoid insider trading liability?

A: Yes, under certain circumstances. On August 15, 2000, the SEC adopted a new insider trading rule, Rule 10b5-1, to resolve an open legal question concerning one of the elements of an insider trading violation. The new rule, which became effective on October 23, 2000, also sets forth certain specific defenses for persons who claim that their trades were done independently of any knowledge of material nonpublic information. As a result, as discussed

(Continued on page 15)

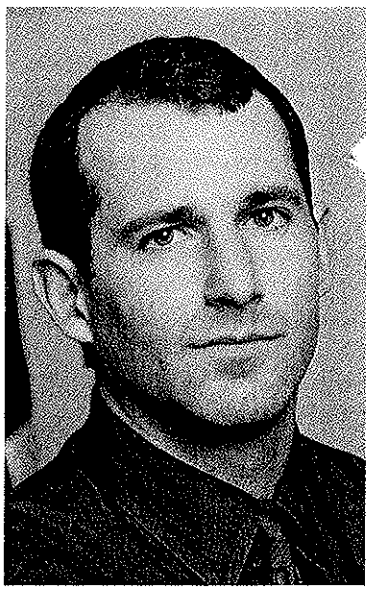
* *In most cases, it was also recommended that a representative of the appropriate SRO or other governing body of the member's firm be consulted to confirm proposed solutions to the problem at hand.*

Internet Fraud: Myths and Reality

One Cybercop's Take on the Truth About the Fight Against Internet Securities Fraud

by John R. Stark, Chief, Office of Internet Enforcement

This article was adapted from a speech made by keynote speaker John Reed Stark, Chief, Office of Internet Enforcement and adjunct professor of law at Georgetown University Law Center, at the 2000 NSCP National Membership Meeting in Washington, DC. The Securities and Exchange Commission 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 Commission or the author's colleagues on the staff of the Commission.



"Kid, the next time I say let's go someplace like Bolivia, let's *go* someplace like Bolivia." Tired of running from the law, Butch Cassidy convinces his sidekick, the Sundance Kid, that success in the bank robbery business requires a change in venue, so the two legendary outlaws relocate from the cliffs of the Rocky Mountains to the small mining towns of southern Bolivia. Butch, who considers himself a master of get-rich-quick schemes, becomes increasingly frustrated at the growing sophistication and zeal of U.S. law enforcement, and he figures that the scattered rural constabularies of South America offer unprotected terrain for accomplished thieves like Sundance and himself. But by the end of that particular movie, Butch and Sundance find themselves on the receiving end of a hail of Bolivian army gunfire.

(Continued on page 2)

Inside

MYTHS OF INTERNET FRAUD
(Continued from page 1)

Butch had miscalculated; it seemed that no matter where he practiced his trade, the long arm of the law caught up with him.

Modern day stock swindlers probably look at Cyberspace the same way Butch Cassidy looked at Bolivia, believing that over the borderless, infinite plains of the Internet they might fly undetected beneath law enforcement's radar. Indeed, as technology continues to expand investors' access to market information and opinion, the Internet continues to offer intriguing new opportunities for con artists and securities cheats to exploit unsuspecting investors. These 21st century con men, however, are succumbing to the same pipe dream that lured Butch Cassidy. Be it Bolivia or Bolivia.com, a well-armored posse lies in wait for the outlaws.

That the Internet provides a safe haven for stock cheats is just one of the many current fallacies about online securities fraud, fallacies that are given credence by the statements of overly pessimistic commentators and pundits. Clearly, as the news media struggles to fill more and more air time and more and more column inches, the hype surrounding Internet fraud continues to escalate.

Rather than perpetuate what I feel are false impressions, today I intend to attack these Internet myths by carefully examining the development of the SEC's Internet enforcement program over the past five years. In particular, I want to draw from the SEC's 200-plus Internet-related securities fraud actions, court cases charging hundreds of entities and individuals with violations of the federal securities statutes and regulations.

There is no doubt that interest in the regulation of securities transactions on the Internet has grown significantly in the past several years. For five years, I've taught a course at Georgetown University Law School called "Securities Law and the Internet." When I began teaching, the SEC had only brought two Internet-related enforcement actions; now we've brought more than 200. Back then, there were about 16 online brokerage firms; now there are more than 160. Even more amazing is the sheer number of Internet-related regulations, interpretive releases, no-action letters and white-paper studies published by the Commission. A unique body of case law is even in the stages of early development in the field of Internet securities fraud. Although in many ways the Internet still remains akin to the Wild West, we are starting to see some sophisticated cities sprouting up where once there were only sagebrush and mining camps.

Before I go on, I want to say a few quick words about the benefits of the Internet for investors. Regulators will always be concerned about protecting investors from online pitfalls, but too often, people forget that the Internet has, for the most part, been a tremendous boon to investors. This is something regulators and other law enforcement authorities must never, ever overlook.

First and foremost, consider that the Internet has fostered direct communication among market participants. On the Internet you will find short-sellers, retail traders, long-term shareholders, business competitors, market analysts, brokers, fund managers, and just about every other conceivable type of market participant, all coming together in one forum for the first time in history. Then there are the many bytes of market information available at a user's fingertips – just about any kind of information you might want to know, from basic price and volume data to more technical stochastic data to the most detailed minutiae of a company's management. It is all available on the Internet 24 hours a day, 7 days a week, from just about anywhere in the world. The Internet's virtual conference room has more than enough space to permit everyone to gather information, exchange ideas and craft informed

(Continued on page 17)

2000 Membership Meeting Workbook Available

The NSCP 2000 National Membership Meeting Workbook, a three-volume collection of written materials provided by each panel moderator, is now available. Some outstanding features of this valuable compliance resource are:

** Analysis of issues raised by employment contracts and non-compete agreements*
** Item by item explanations for completing the new Form ADV and proposed Part II*
** The tricks of the trade when monitoring the bulletin board activities of your employees*
** The "Do's & Don'ts" of soft dollar compliance*
** Various solutions to the challenge posed by supervising representatives in remote locations*
** Checklist for automating investment adviser trading compliance*
** Depiction of the legal landscape after Gramm-Leach-Bliley*
** Preparation for regulatory review of an investment adviser - before, during and after*
** Guidance on obtaining and surveilling for best execution*
** Selected regulatory issues for investment adviser hedge fund operation*
** Laundry list for mutual funds' compliance with anti-money laundering rules*

To order a copy of the NSCP 2000 National Membership Meeting Workbook, visit: www.nscp.org. Scroll down; the link is at the bottom of the page.

PRICES: Members $200;
Member Associates $220;
Non-Members $250. Delivery cannot be guaranteed after
January 31, 2001. Please allow 2 to 3 weeks for delivery. Return check and order form to:
NSCP WORKBOOK,
P.O. Box 351, 24 Millerton Rd.,
Lakeville, CT 06039.

MYTHS OF INTERNET FRAUD
(Continued from page 2)

decisions. Unfortunately few filters separate the good information from the bad – which brings us to the risky aspects of the Internet.

Along with the good comes some bad, like securities fraud. Of course, fraud involves only a small minority of Internet users, a small group of people on the Internet trying to exploit Cyberspace to take advantage of investors. Over the past several years, we have focused our Internet program on this small cadre of con artists. In fact, almost all of our Internet enforcement actions allege some type of fraudulent conduct. In other words, in the vast majority of enforcement actions we have brought, someone is lying, cheating and stealing from someone else.

Much of what you read in the newspapers and hear on television spotlights the dark side of the Internet, demonizing it, overstating potential dangers, sensationalizing isolated scenarios for ratings and readership. What we now have is a glut of misinformation and exaggeration, and as a result, the hype surrounding Internet fraud begs for clarification.

My purpose today is to address the hype and deflate it by carefully looking at the now substantial SEC file of Internet enforcement cases. I will break my discussion into four separate parts; each one focused on what I feel is a primary negative myth about online securities fraud enforcement.

Myth#1: The Same Old Scams

Myth#1: "The Internet has created a new kind of securities fraud never seen before." That is completely wrong. What we see in Cyberspace are the same old scams – pump-and-dump schemes, pyramid schemes, Ponzi schemes, prime bank schemes – simply packaged in a different medium.

Like some non-Internet frauds, Internet schemes can be exotic. Some of the early cases we brought involved eel farms, coconut plantations, even investment in underwater islands and fictional countries. Like non-Internet frauds, Internet frauds can be complicated, promising rich returns from foreign trading programs or so-called prime bank investment vehicles, programs that con artists claim generate income through the trading of illusory bank debt instruments on secret, underground exchanges.

Finally, there are also the pump-and-dump schemes that have plagued U.S. markets for a century. In these schemes, a scammer owning shares in a public company fabricates trades between his accounts and spreads false information about the company in an effort to artificially inflate that company's stock price, finally dumping his or her shares into the market on unsuspecting investors at the peak of the scheme, leaving those innocents holding the bag.

Now here is where some of you might take issue with my premise – because the Internet does indeed allow crooks to spread their false information more quickly, easily, and efficiently, and at little or no cost. The Internet permits con artists to do, with the click of a mouse, what in prior years might have taken dozens, if not hundreds, of highly-trained high-pressure stock salesmen. But whether a stick-up man uses a .22 or a .45, a robbery is still a robbery, and one still approaches it in the same general manner.

At one time, if you wanted to manipulate a company's stock, you probably worked for the company, or you worked at one of the "bucket shops" or "boiler rooms" employed so often in the seventies, eighties and nineties. You were also probably pretty sophisticated, and you understood the intricacies of the financial marketplace, especially the mechanics of securities transactions. Well, today, there are no longer such rigid qualifications for enrolling at Stock Fraud University. These days you can conduct your own private market manipulation without any help from

(Continued on page 18)

MYTHS OF INTERNET FRAUD
(Continued from page 17)

the company, without any help from brokers or promoters, and with only a modicum of knowledge regarding how the stock market works. All you need is a computer and a modem (and sometimes you don't even need that much).

Take the recent SEC enforcement action involving an over-the-counter bulletin board company called NEI Webworld, Inc., or NEI for short. In November 1999 we allege a group of twenty-something friends in the Los Angeles area decided to buy some NEI stock. NEI was what many would refer to as a shell company both metaphysically and physically: metaphysically because NEI had undergone Chapter Seven liquidation and owned no assets; physically because the company existed only as a name on the side of an empty, derelict building. Why was NEI still even trading? Sometimes shell company stocks continue to trade on the over-the-counter bulletin board and in the National Quotation Bureau's printed price quotations (the so-called "pink sheets") long after their businesses have run their course. This one, NEI, was trading at $.10 to .12 a share at the time we allege that this group of West Coast cronies started buying its stock.

After a week or so of quietly purchasing NEI shares through a series of domestic and offshore brokerage accounts, the SEC alleges that this group, led by a man named Arash Aziz-Golshani, posted on various Internet message boards that NEI was going to merge with LGC Wireless, a private company with active business operations in the San Francisco Bay area. We allege that the messages, known on the Internet as "spam" or repetitive junk mail, touted the purported merger with LGC Wireless, even providing an actual link to LGC's homepage. The spam promised that NEI's share price was going to move up between $5 and $10 a share in the next few days. The SEC alleges that they not only spread these messages on the boards numerous times under different message board "user names," they also created aliases and responded to these messages in the guise of ordinary investors in order to create the appearance of investor interest in the merger.

This spring, Mr. Aziz-Golshani pled guilty to a count of criminal securities fraud and a count of conspiracy; another accomplice, Hootan Melamed, pled guilty to a conspiracy count. They are still awaiting sentencing and the resolution of an amended civil complaint alleging that they made close to $700,000 manipulating the stock of NEI and 11 other e-businesses.

The New York Times *ran a front page story on our suit against Tokyo Joe, saying that it raised a host of First Amendment issues... The First Amendment simply does not shield those who publish false and misleading statements with the intent of stealing from investors and it never will.*

The manipulation of NEI shares was done entirely by a third party, meaning no involvement by NEI, and no illicit participation by any licensed professionals, such as brokers, market-makers, transfer agents, etc. Of course, the traditional pump-and-dump scams, where promoters of companies themselves actually facilitate the dissemination of false information, still occur in Cyberspace. Consider the recent and pending action involving Uniprime Capital Acceptance, Inc.

In this enforcement action the SEC alleges that Uniprime Capital Acceptance was a Las Vegas car dealership that was approached by a former carnival worker and felony convict named Alfred Flores, a man who claimed to be an immunobiologist with a degree from the University of Madrid and a vial full of a sure-fire cure for AIDS. The SEC alleges that Uniprime's stock, which had lingered beneath $1 per share, went from $.625 to nearly $8 per share on the strength of a pair of press releases touting this bogus AIDS cure, press releases whose dissemination was made faster, more widespread and more efficient by message board postings and Internet websites. The SEC alleges that Uniprime's website, in addition to displaying copies of the releases, also exhibited fake testimonials from AIDS patients allegedly treated with Flores' remedy. Even after trading in Uniprime's shares was suspended due to questions regarding the press releases' accuracy, their effect was still strong enough to permit Uniprime to sell over $400,000 in stock to investors through private placements. The SEC alleges that Flores, the supposed medical miracle worker behind this remarkable cure, had, in fact, been incarcerated in Colorado for nearly eight years following his conviction for conspiracy to commit murder in 1984.

Again, we have seen this type of alleged stock fraud for decades, but this is yet another example of how the Internet not only enables con men to access investors with ruthless efficiency, but also arms them with tools like websites and message boards to lend their schemes digital-age credibility.

Now, despite my earlier assertion that most Internet frauds remain simply the same old scams, only more slickly produced, courtesy of the World Wide Web, there are some new variations that have emerged only during the past year or so. Let's examine four of these recent fraud types: momentum sites, stock recommendation sites, impostor hoaxes, and insider trading.

- Momentum Sites

"Momentum trading" ("Momo") is a variation on the standard pump-and-dump that involves websites or e-mail services that encourage members to buy a specific stock, at a specific time, to create a concentrated, short-term demand. The stock is usually a thinly-traded microcap,

particularly susceptible to market movements, with not much in terms of operations or information in the marketplace. The concept is that if enough subscribers follow the "Momo" group leader's recommendation, the stock is going to rise, and the leader is frequently going to start to sell the shares he bought previously and take profits. The spike hits, and the price drops. This typically occurs in just a few hours.

One of the most recent cases we brought in this area involved a website called Fast Trades, operated by a group of Georgetown law students (none of whom, incidentally, had taken my class). And we ended up suing them during the semester I was teaching "Securities Laws and the Internet."

Douglas Colt, ringleader of the group behind the Fast Trades site, searched for the vulnerable, thinly-traded microcap stock. Among Colt's first picks was American Education, trading at about $1 a share. First, he bought the stock cheap. On March 5, 1999, Colt started buying the stock at 10:47 a.m. and continued until about 2:19 p.m., buying up about 19,000 shares. Next: the pump. We alleged that he then started hyping the stock on his momentum trading site and on various message boards. Then, he announced it as his "momentum" pick on his website. By 2:45 p.m., when Colt posted the stock on fast-trades.com, 100,000 shares had been traded, and the stock reached a high of about $10. Finally, the dump. We alleged that the perpetrators entered a limit order of $6.50; as soon as the stock hit that price, their sales began to take place, and they made a quick profit. In this case, for a couple of days' work, we alleged Colt made $41,000. By the end of Colt's involvement, the stock had dropped to $3.25 a share, stinging many investors.

Fast Trades was an interesting case because it involved a type of scalping, where you sell into your own buy recommendations time after time. Your disclaimer might say that you *may* do that, or that you reserve the *option* to do that, but the reality is that you're doing it every single time. We also alleged that the Fast Trades' postings on the Internet were false, and the track record that they set forth was false. They had 9,000 subscribers, and we alleged they made $345,000 in illegal profits.

The Fast Trades enforcement action demonstrated one additional thing about the Internet: securities scam artists want the world to hear their false information, so that investors will buy into their schemes and their profits will go up, and the more people who know about those schemes, the better. Well, unfortunately for them, the SEC is not only part of the neighborhood watch program but is also part of the listening audience. This guy Colt had such hubris that he even boastfully posted an online blueprint of his 11-point plan to run up the price of a stock, ending with his own personal observation that a good Momo site operator can "dump all of your stock to [its] idiot subscribers . . . and laugh all the way to the bank."

- Stock Recommendation Sites

Here, we have so-called "stock gurus" who give instant advice on when to buy or sell stock, providing chat rooms, e-mail, and even pager notification services. The operators make their money through subscription fees. They'll promise you anything and everything from quick riches to an improved golf game. The violations here are of a much broader variety: false and misleading advertising (which could also trigger FTC rule violations), broker-dealer registration issues, investment adviser registration issues and touting violations (in which people illegally take undisclosed payments for favorable recommendations and promotions about a company's stock). The biggest SEC enforcement action of this kind involves a man named, Yun Soo Oh Park, or, as he was better known online, Tokyo Joe, who ran a chain of burrito restaurants in Manhattan. This action remains in litigation (as are some of the other actions mentioned today) so please understand that whatever I state are SEC allegations only.

Tokyo Joe was a rather well-known online "investment guru," charging subscribers $100 to $200 dollars per month for stock picks. We allege that Tokyo Joe was doing some scalping, and that at least one issuer had been providing compensation to him; we allege that he made material misrepresentations about his track record, and we allege that he made over 200 false and misleading statements on his website.

The New York Times ran a front page story on our suit against Tokyo Joe, saying that it raised a host of First Amendment issues. I don't see this as a defense, and when Tokyo Joe filed his motion to dismiss our complaint, the judge agreed, quickly dismissing Tokyo Joe's argument. The First Amendment simply does not shield those who publish false and misleading statements with the intent of stealing from investors and it never will.

- Impersonation Hoaxes

Next we have "impersonation hoaxes," where an Internet user posts false information by creating a fictional press release. The "impersonation" angle comes into play because, in some cases, scammers go to great lengths to disguise their phony releases as the products of legitimate news organizations, in an attempt to make the news they tout more credible and its market impact greater. Some of the most notorious SEC enforcement actions involve imposters. I want to tell you about four of them.

First, a man named Gary Dale Hoke posted anonymously on a message board and set up a phony, anonymous web page stating that a California company, PairGain Technologies, was going to be bought by an Israeli company. The page was designed to resemble a Bloomberg news release. The sham page had a forward-looking statement disclaimer at the bottom, which most

(Continued on page 20)

MYTHS OF INTERNET FRAUD
(Continued from page 19)

Bloomberg stories don't have, and that might have been a clue to some observant Internet users. But Hoke's sham Bloomberg news release resulted in a significant movement in the price of PairGain's stock that day, because many investors believed it to be true. But we tracked him down, he was arrested, criminally and civilly charged, and was sentenced to five years probation and ordered to pay $93,000 in restitution. Perhaps because he was caught so thoroughly off-guard by the effectiveness of his own scheme, he didn't even manage to dump his own shares for a profit, although many other innocent investors bought into his fantasy.

Another case: *SEC* v. *Leszek Zbierajewski*. This man posted a false PR Newswire release announcing an $89 million dollar alliance between bid.com and America Online. He made his posting look like a real PR Newswire press release, announcing that this deal was going to take place pretty quickly. Many message board posters challenged him: "you're going to jail just like Gary Hoke, because that's a lie! There's no $89 million dollar alliance with AOL, you just made that up!" And he withdrew the posting twenty minutes later saying, "I'm sorry, that was news I hoped would happen, I was hoping they had a deal with AOL, I was just letting off some steam." But it was too late – he'd already had an impact on the market and the SEC filed an enforcement action against him for his fraud. False information in the market for only a few moments can still have a significant effect on the price of even a widely-traded stock, as our next case illustrates.

Third: Fred Moldofsky. This case, involving the stock of Lucent Technologies, is still active (in both SEC and a criminal proceedings), so I'll be brief in my remarks concerning our allegations. On the afternoon of March 22, 2000, Moldofsky allegedly posted message board rumors that Lucent would not meet its quarterly earnings estimates. That evening, we allege he posted a fake PR Newswire announcement and other messages repeatedly stating that Lucent's earnings were going to be bad. We allege that he took language from an old Lucent press release and just copied it. We caught him within days; he was arrested and charged by both the SEC and criminal authorities.

This is an example of an alleged "cybersmear," in which people publish information to drive down the price of the stock, not a scheme to artificially inflate the price, as in a pump-and-dump scheme. Cybersmears are interesting, because even if they do not have an impact on a company's stock price, people hear rumors, company employees get upset, analysts might take note, customers might start questioning partners. Everyone in the company can suddenly start to have questions when false rumors are spread on the Internet, because we all know that sometimes rumors are true.

Finally: the Emulex hoax. The Emulex hoax is a recent enforcement action that you may have read about and is still active (in both SEC and a criminal proceedings). Emulex involves some actual trading and another bogus news announcement. In August, Mark S. Jakob, a community college student who worked for a wire service called Internet Wire, sold short 3,000 shares of a Costa Mesa, California high-tech company called Emulex Corporation, at about $80 a share. Within a week, the shares went up to $133 per share. We found that Mr. Jakob was $97,000 in the hole, and as I am sure you understand, when you're selling short, the potential losses are limitless. The higher the price goes, the deeper you go into the red.

We allege that one evening, Mr. Jakob sent an e-mail to Internet Wire containing a fake press release, purportedly from Emulex, stating that the company announced revised earnings showing a loss instead of a profit, that the SEC had launched an

investigation into its accounting practices, and that its CEO had stepped down. The release went out over Internet Wire, in spite of company procedures for confirming the authenticity of releases. Bloomberg picked it up, as did Dow Jones, and suddenly everyone was talking about it, including Jim Cramer of TheStreet.com. And it looked real.

It was 9:30 a.m. when Internet Wire disseminated the press release. At 10:13 a.m. the newswires started picking it up, and suddenly there were headlines. Between 10:13 and 10:29 a.m., 2.3 million Emulex shares were traded and the price plummeted to $61 a share. That's a $2.2 billion dollar market cap loss in just sixteen minutes. Nasdaq halted Emulex's trading at 10:29 a.m., and the stock resumed trading once the company denied the phony report. At the time trading resumed, the stock price returned to about $105 per share.

What did Mr. Jacob do in the course of about 15 minutes? We allege that just before the trading halt, he covered his short position and made a profit of $54,000. But we also allege that he didn't stop there. We allege that he knew that the information he released would be exposed as a hoax, and that he bought some Emulex shares hoping to profit on the upswing. We allege that he sold the stock he purchased, at a profit of over $186,000 at a total profit: $241,000 – not bad for a guy who was $97,000 in the hole the day before. Mr. Jakob was arrested within a week and faces up to 15 years in prison if convicted.

- Insider Trading

Now for the last variation, insider trading. Here's an interesting case: SEC v. Freeman, March 2000. This was the first major Internet insider trading SEC enforcement action. In this action which remains in litigation and in criminal court as well, the SEC alleges Mr. Freeman, a temporary nighttime word processor at a pair of major Wall Street brokerage firms, misappropriated information concerning 23 different transactions. The SEC alleges that Mr. Freeman tipped at least 10 others, and also passed those tips to still others in Internet chat rooms, one of which was called The Bren. We allege that his direct and indirect tippees made over $8 million in profits. He was arrested and was also charged civilly by the SEC. Fifteen other people were also charged as part of the insider-trading ring.

Myth #2: Efficacy

Myth #2: "There is simply no way to send a message to Internet fraud artists that we won't tolerate their wrongdoing." That statement is also 100 percent untrue. If you look at the groups of enforcement actions we've filed together, what we call "sweeps," you'll see that we've gotten the message out that we are going to be pretty aggressive on the Internet. In October 1998, we targeted unlawful touting, the practice of receiving payment for investment opinions without investors knowing the opinions were bought and paid for. We filed 23 actions against 44 respondents and defendants who had touted over 235 microcap stocks. We looked at their spam, newsletters, message board postings, and websites.

How can you file a case where no money has been lost? Very easily. The Internet offers an investigator an incredible and resplendent evidentiary trail... Law enforcement officials and regulators now have the opportunity to review a fraud as it develops in front of their own eyes.

We went back to that same "street corner" in February 1999, filing four more actions against touters who had received money and shares of stock to unlawfully promote companies online. In May 1999, we targeted phony offerings on the Internet and brought 16 enforcement actions against 26 companies and individuals. We called that one a "preemptive strike" because five of the cases were filed before any money was lost.

How can you file a case where no money has been lost? Very easily. The Internet offers an investigator an incredible and resplendent evidentiary trail. You don't have to wait for someone to complain, you can see the fraud in front of you. You don't have to wait for someone to get ripped off, you can act beforehand. You don't have to rely on victims coming forward, you can review the phony offering without ever contacting anyone. And that, ladies and gentlemen, remains one of the marvelous aspects of the Internet, from an enforcement perspective. Law enforcement officials and regulators now have the opportunity to review a fraud as it develops in front of their own eyes. The Internet offers a plain view, or a window if you will, into the scams, all visible from any SEC desktop computer.

Last month in our most recent sweep, we targeted market manipulations and filed 15 enforcement actions against 33 companies and individuals. All of these were pump-and-dump scams involving more than $1.7 billion in market cap movement because of the false information that these people and others were spreading. We are seeking about $10 million in disgorgement in the course of those actions.

These sweeps are a wonderful means of sending the message to online scam artists that we mean business. And we're going to keep hitting the con artists over and over again. We're never going to stop. And although we cannot mirror the speed of a T1 line, we will make every attempt to move just as quickly.

Myth #3: Territory

Myth #3: "The Internet is infinite territory and impossible to surveil." The reality is just the opposite. First of all, we have a five-prong approach toward Internet fraud, increased surveillance to find fraud at

(Continued on page 22)

MYTHS OF INTERNET FRAUD
(Continued from page 21)

an early stage, cultivation of self-policing to open channels of communication with the public, educational initiatives to create more savvy investors, aggressive prosecution to deter fraud, and stepped-up liaison work to insure that we leverage our resources through cooperation with other agencies. This effort is spearheaded by the Office of Internet Enforcement, where I work.

The Enforcement Division also has a surveillance squad called The CyberForce, an automated Web search engine, an Enforcement Complaint Center that gathers messages from the public reporting wrongdoing (more than 400 every single day), and dedicated investigative branches all over the country that do only Internet fraud investigations. The CyberForce, made up of attorneys, accountants and analysts, leads our surveillance efforts, looking at the Internet usually every day.

But there really is no need to look daily – the surveillance part of Internet enforcement is very simple. Because you see, unlike hackers trying to tamper with the energy grid or crackers clandestinely trying to intrude into the computer networks of public companies, securities scam artists essentially want to be found. Internet scam artists (like all scam artists) require a wide audience to review their false information, invest in their stock recommendation or send money to invest in their investment opportunity. The more people who receive the false information, the more investors will likely buy into their scheme. The larger the investor audience (which includes SEC enforcement staff by default), the better chances of finding victims.

For example, during the course of a day I might visit a potentially fraudulent website, the site may drop a "cookie" on me or even grab my e-mail address, depositing me on their "sucker" list forever. So when the scam artist sends out his or her next bulk e-mail it will land in my e-mail box. This means that I'm conducting surveillance right now. When I go back to check my e-mail, there will be a pile of spam. To the con men I say: thanks for sending me the evidence I need, I appreciate it. I was doing a speech this morning and I couldn't be on my computer to look for you.

Myth #4: Resources

Myth #4: "The SEC's limited resources cannot possibly locate all of the Internet con artists." The Internet may indeed be potentially infinite territory, but the truth is, we're not alone, we never have been, and we never will be. We've got a virtual community of people on the Internet who remain extremely enthusiastic to report any frauds they've seen. I've received 400 e-mails per day in the last two weeks, which means more than 400 Internet users each day take the time to report suspicious conduct to us in our Enforcement Complaint Center, which we set up in June 1996. I have been in charge of that program since 1994: I set up the complaint center without knowing what would happen. Initially, I didn't realize so many people would be so active; the public has been a tremendous source of leads, and I have no doubts that the vigilant Internet community will remain the primary source of leads in the future.

Conclusion

That concludes my discussion of some of today's prevailing myths concerning Internet fraud. I hope I have convinced you that the realities of the cyberfraud business are not quite as bad as you might think. Now let's return to Bolivia for a moment.

Legend has it that it was sometime around 1904 when the real Butch Cassidy and Sundance Kid began their Latin American bank robbery spree, making it almost 100 years ago that the two outlaws concocted their southward journey. In hindsight, Butch fell trap to the illusion that Bolivia was a sparse and uncharted landscape offered the ideal landscape for criminal success.

Today's market manipulators and investment cheats may possess a similar delusion – that the Internet shares some of Bolivia's allure only on a far grander scale, a jurisdiction with boundless unmarked topography, offering a cheaper, faster and easier opportunity for thieves to commit securities fraud. But what today's cybercrooks fail to realize is that the reality is very much the antithesis. Rather than create a new frontier for scam artists, the Internet has for the first time in history put investment scams in plain view, making frauds easier to surveil, easier to track, and ultimately, easier to catch.

Historians claim that it was not until 1908 that the local authorities finally caught up with Butch and Sundance in a rented hut in San Vicente, a town in southern Bolivia, which means the duo enjoyed nearly half a decade on the lam, a lifetime measured in Internet years. Nowadays, during the current prenatal stage of the information technology era, a cyberthief may not even last on the lam for three days, let alone three years – just ask Gary Hoke, Leszek Zbierajewski, or any of the others prosecuted by the SEC.

These SEC defendants (and many of the others who now number in the hundreds) would probably tell you that ever since they decided to use the Internet to take advantage of unsuspecting investors, unlike Butch and Sundance, far more than just raindrops keep falling on their heads. These defendants will tell you that along with those raindrops can come a lot more to worry about, like SEC injunctions, monetary penalties, disgorgement, penny stock bars, officer and director bars and sometimes even criminal prosecution.

For a better understanding of the world of enforcement, you can visit our website, at www.sec.gov and find summaries of all the cases, including those that were part of one of our Internet sweeps. And remember, if you know of an investment fraud or other violation of the federal securities laws, all you have to do is drop us a note at enforcement@sec.gov. ❑