United States General Accounting Office

GAO

Testimony

Before the Permanent Subcommittee on Investigations
Committee on Governmental Affairs
U.S. Senate

**For Release on Delivery
Expected at
1:30 p.m. EST
on Monday
March 22, 1999**

SECURITIES FRAUD

The Internet Poses Challenges to Regulators and Investors

Statement of Richard J. Hillman
Associate Director, Financial Institutions
and Markets Issues
General Government Division

Securities Fraud: The Internet Poses Challenges to Regulators and Investors

The Internet is a global network of computers that ties together an estimated 153 million users worldwide and is providing the basis for a rapid expansion in electronic commerce. The rapid growth of Internet commerce is also significantly transforming the U.S. securities industry. For example, in 1998, approximately 22 percent of all securities transactions were conducted over the Internet compared with virtually no such transactions in 1995. According to industry observers, the Internet is popular among investors because it allows them to buy and sell securities from their personal computers, lower trading commissions, and gain ready access to market research.

Unfortunately, the Internet also provides fraudulent operators with a new and efficient medium to defraud investors of millions of dollars. Fraudulent operators find the Internet attractive because they can instantly communicate with millions of potential victims—via professionally looking websites, that appear to offer legitimate investment information, on-line newsletters, or e-mail—at far lower costs than traditional means of communication, such as the telephone. In addition, the Internet makes it easier for fraudulent operators to remain anonymous and commit crimes from nearly any location in the world and thereby evade U.S. regulatory and law enforcement authorities.

According to Securities and Exchange Commission (SEC) officials, as the Internet continues to expand rapidly, opportunities for securities frauds increase as well. For example, the number of E-mail complaints submitted to SEC, many of which allege potential Internet frauds, soared from about 10 to 15 daily in 1997 to between 200 and 300 daily in early 1999. According to SEC, the types of frauds committed over the Internet are generally traditional securities frauds. In one scheme, individuals who own a company's securities spread positive but false information about the company to increase investor interest and drive-up the price of the securities. The individuals then sell their securities at a quick profit, while later investors face large losses when the price of the inflated securities declines.

SEC has established an office to coordinate the agency's response to Internet fraud, provide training to SEC staff on monitoring the Internet, and develop guidance for SEC staff to follow when investigating Internet fraud cases. SEC has also (1) developed education programs to warn investors about the risks associated with Internet investing and (2) initiated 66 enforcement actions since 1995 to punish alleged perpetrators of Internet securities frauds. Nearly half of the 50 state securities regulatory agencies we surveyed have also developed specific programs to

monitor the Internet for potential frauds and penalize violators of state securities laws.

However, SEC and state regulatory programs to combat Internet securities fraud are new and face significant challenges that could limit their long-term effectiveness. In particular, the potential exists that the rapid growth in reported Internet securities frauds could ultimately place a significant burden on the regulators' limited investigative staff resources and thereby limit the agencies' capacity to respond effectively to credible fraud allegations. Moreover, the regulators face challenges in developing a coordinated approach to combating Internet fraud and educating a wide audience about the potential risks of Internet investing.

Ms. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss Internet securities fraud and regulatory efforts to combat this growing problem. The Internet is a global network of computers that ties together an estimated 153 million[1] users worldwide and is providing the basis for a rapid expansion in electronic commerce. According to one industry research firm,[2] total U.S. business trade on the Internet reached $43 billion in 1998 and is projected to soar to $1.3 trillion by 2003. The rapid growth of the Internet is also significantly transforming the securities industry in the United States. An industry study,[3] reported that approximately 22 percent of all retail U.S. securities trades were conducted over the Internet in the first half of 1998, which was significant given that there was virtually no on-line trading in 1995. The industry study projected that the total number of on-line brokerage accounts will nearly triple from about 5 million in 1998 to over 14 million in 2002.

Securities industry observers and participants cite several benefits that the Internet provides to investors, which account for its growing popularity. In particular, the Internet permits investors to place buy and sell orders from the convenience of their personal computers and can lower trading commission fees charged by full-service brokers. By accessing broker-dealer webpages, investors can also gain access to stock market research that previously was not readily accessible to the investing public. Moreover, the Internet also allows investors to obtain immediate access to price quotes on securities or mutual funds.

Unfortunately, the Internet also provides several advantages to fraudulent operators who are using the new medium to defraud investors of millions of dollars. First, the Internet provides fraudulent operators with the ability to communicate electronically with millions of potential victims at a far lower cost than traditional means of communication, such as the telephone or mass mailings. Fraudulent operators can communicate with investors over the Internet through professionally designed webpages that may appear to offer legitimate investment information, on-line investor newsletters, chatrooms, or mass E-mailings (called "spam"). Second, fraudulent operators can use technology available on the Internet that

[1] NUA Internet Surveys: How Many On-line? January 1999, NUA Ltd.

[2] U.S. On-line Business Trade Will Soar To $1.3 Trillion By 2003. December 1998, Forrester Research, Inc.

[3] Broker Watch. Investorguide.com, Inc.

makes it easier to hide their identity and thereby evade regulatory authorities. Third, fraudulent operators with Internet access can quickly initiate investment scams from virtually any location in the world thereby making it difficult for federal and state regulators to catch and prosecute violators or obtain compensation for victims.

As you requested, my statement will

- provide information about the incidence and types of securities frauds perpetrated over the Internet,
- describe Securities and Exchange Commission (SEC) initiatives to combat Internet securities fraud,
- provide information on the penalties that have been imposed on individuals found to have committed Internet securities frauds,
- present information from state securities regulators about state efforts to control Internet securities fraud, and
- identify potential challenges facing SEC and state regulatory initiatives in combating securities fraud over the Internet.

In summary, our work to date indicates that:

- SEC and state regulatory officials generally agree that as the Internet continues to expand rapidly, opportunities for securities frauds are growing as well. One rough indicator of the growth in Internet securities fraud is the number of public E-mail complaints that are submitted to SEC's Internet website. The number of such E-mail complaints, many of which allege potential Internet securities frauds, soared from 10 to 15 daily in 1996 to between 200 and 300 daily in early 1999.
- According to SEC, the Internet provides a new medium to perpetrate traditional investor frauds, such as stock price manipulation schemes. However, some securities frauds appear unique to the Internet environment, such as the reported illegal copying of legitimate broker-dealer webpages for the purposes of defrauding unknowing investors.
- SEC has responded to the growing Internet fraud problem by, among other things, creating the Office of Internet Enforcement (OIE) to coordinate the agency's efforts to combat Internet fraud, providing training to SEC investigative staff on monitoring the Internet, and preparing guidance for

SEC staff who are investigating potential Internet frauds. In addition, SEC has established programs to educate investors about the risks associated with Internet securities frauds, such as posting relevant information on its website.

- Since 1995, SEC initiated a total of 66 enforcement actions against alleged perpetrators of Internet securities frauds. As of February 1999, 32 of the 66 cases had largely been concluded, with violators generally required to (1) pay civil money penalties or (2) refrain from further violations of the securities laws. However, in 2 of the 32 concluded cases, state or federal criminal enforcement authorities prosecuted violators and obtained criminal convictions or prison sentences for 7 individuals.

- Over the past several years, nearly half of all state regulatory agencies have established specific programs to combat Internet frauds that violate state securities laws. Although many state agencies have initiated enforcement actions to prevent further violations of state law, officials from these agencies told us that in some cases violators may continue committing the fraudulent activity in other states.

- SEC and state regulatory agency programs to combat Internet securities fraud are new and face significant challenges that could limit their effectiveness in the long-term. In particular, the potential exists that the rapid growth in reported Internet securities frauds could ultimately place a significant burden on the regulators' limited investigative staff resources and thereby limit the agencies' capacity to respond effectively to credible fraud allegations. Moreover, the regulators face challenges in developing a coordinated approach to combating Internet fraud and educating a wide audience about the risks associated with Internet investing.

Due to time constraints, we focused our analysis on SEC and state agency regulatory efforts to combat Internet securities fraud rather than other securities regulators that may also play a role, such as the National Association of Securities Dealers (NASD), the New York Stock Exchange (NYSE), and the Commodities Futures Trading Commission (CFTC). However, we did meet with officials from these organizations to obtain a general understanding of their regulatory efforts.

To meet our objectives for this work, we interviewed SEC officials from OIE, Division of Market Surveillance, Office of Investor Education, and the San Francisco District Office. We also obtained information from SEC on the outcomes of the 66 Internet securities fraud cases and reviewed the data contained in a random sample of 100 complaints received by the SEC and referred to SEC regional and district offices and other federal

agencies. In addition, we met with officials from the Federal Trade Commission (FTC), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the White Collar Crime Center,[4] and the North American Association of Securities Administrators (NAASA) to discuss their roles in monitoring and combating Internet securities fraud. Finally, we (1) surveyed officials from all 50 state securities regulatory agencies to obtain their views on Internet securities fraud and efforts to control this growing problem and (2) met with officials from three on-line broker-dealers to discuss securities fraud and related issues. We did our work between October 1998 and March 1999 in accordance with generally accepted government auditing standards.

Regulators Report That Internet Securities Frauds Are Increasing

There are no comprehensive statistics available on the incidence of securities frauds committed over the Internet. However, SEC and other federal agency officials we contacted said that Internet securities fraud is an emerging problem, which will likely grow as the use of the Internet continues to expand worldwide. The data available from state securities agencies also suggest that Internet securities fraud is increasing. According to SEC, the growing number of frauds committed over the Internet are types that are generally well-established in the securities industry. For example, in one common scheme, an individual who owns a large number of shares spreads positive but materially false information about a company over the Internet. This information drives up the company's stock price and the individual makes a profit from the sale of these stocks at the expense of other investors (commonly referred to as "pump and dump" schemes). We also identified some frauds that appear unique to the Internet environment, such as the reported illegal copying of legitimate broker-dealer websites for purposes of defrauding unknowing investors.

The Volume of Public E-mail Complaints About Internet Securities Fraud Suggests an Emerging Problem

One rough indicator of the growth of Internet securities fraud is the number of complaints that SEC has received through its E-mail complaint system, which was established in June 1996. According to SEC, the public submitted about 10 to15 complaints daily in 1996 via the E-mail system with the number rising to about 120 daily through September 1998. After SEC publicly announced a crackdown on Internet securities fraud in October 1998, SEC officials said the number of daily E-mail complaints soared to 200 to 300 daily and has continued to run about this range in early 1999. However, it is important to note that the volume of daily E-mail

[4]The National White Collar Crime Center is a unit within the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance that provides services, such as information sharing, case funding, training and research to local and state law enforcement, prosecution, and regulatory agency members.

complaints submitted to SEC has several significant limitations as a measure of the extent of Internet securities fraud. For example, investors who are unaware that they have been defrauded would not likely submit E-mail complaints to SEC. In addition, SEC receives E-mail complaints that do not involve potential violations of the securities laws and some complaints may allege securities frauds that do not involve the Internet.

Other organizations and state regulatory agencies have also reported a significant number of public complaints regarding potential securities fraud committed over the Internet. NAASA—the organization that represents state securities regulatory agencies—received about 350 securities-related complaints involving the Internet over a 4-week period in October 1998, when NAASA first established an E-mail complaint system. Officials from securities regulatory agencies in 37 of the 50 states surveyed told us that they collectively received over 1,400 complaints related to potential Internet securities frauds last year. Generally, states reported receiving no such complaints in 1996.

The Internet Provides a New Medium to Perpetrate Traditional Securities Frauds

SEC officials told us that the Internet provides a new medium for perpetrating fraudulent schemes that are well-established violations in the securities industry. Some of the fraudulent schemes are violations of the Securities Act of 1933 and the Securities Exchange Act of 1934. For example, one commonly employed fraudulent scheme involves disseminating materially false information via spam, websites, on-line newsletters, or other means about small companies that have issued thinly traded securities. The transmission of materially false information—such as false statements about a company's financial condition—over the Internet provides instant access to millions of potential victims at far lower costs than traditional means of perpetrating scams, such as the telephone or mass mailings.

According to SEC officials, one reason fraudulent operators spread false information about companies and their securities is to increase investor purchases of the securities, thereby increasing share prices. Frequently, the fraudulent operators already own a large number of these securities and are able to make quick profits by selling their securities as prices increase. By contrast, investors who purchase securities on the basis of false information may experience significant and rapid losses when the perpetrators sell their large positions. For example, in one case, SEC alleged that the defendants encouraged discussion about a company on Internet news groups and disseminated information that materially misrepresented the state of the company's technology, commercial viability, and existence of purchase orders for equipment. SEC further

alleged that while continuing this scheme the defendants sold the company's securities for more than $3 million.

SEC identified fraudulent operators who frequently provide compensation to, for example, on-line newsletters in the form of securities or cash to further these schemes. The newsletters publish the false information about companies or claim to provide "objective analysis" about the promising prospects for the securities without disclosing the compensation provided to the newsletter in exchange for publishing this positive information, a practice known as "touting." Touters often sell their shares in the company immediately following their recommendations, which is a deceptive practice commonly referred to as "scalping." In October 1998, SEC announced a nationwide crackdown on Internet touting, charging a total of 44 individuals or companies with engaging in the practice. In February 1999, SEC continued its Internet fraud crackdown and charged another 13 individuals or companies. We discuss SEC's enforcement activities in more detail later in this statement.

The sale of unregistered securities on the Internet is a problem reported among the states we contacted. In one case, Connecticut securities officials found that a prepaid cellular telephone company was advertising falsely over the Internet that it would sell limited liability partnership interests for a minimum price of $5,000. Rather than using these funds to create a cellular telephone network in the Boston area as advertised, state regulators believed that the money may have been diverted to the company's owners. Other state securities regulators have reported the illegal sale over the Internet of stocks in offshore gambling enterprises, time travel technology, Hollywood movie theme restaurants, and air-conditioning and helicopter production companies. Financial losses suffered among victims of illegal securities sales reportedly ranged from $18,000 to over $100 million.

Other Internet securities frauds identified by federal and state regulators include initial public offerings and prime bank note schemes.[5]

The Internet Also Provides Opportunities for a New Type of Securities Fraud

Although the Internet generally provides a new medium to commit traditional securities frauds, it has also provided opportunities for some new fraudulent schemes. For example, officials from a licensed, on-line broker-dealer in California told us that in May 1997, the company's website

[5]In a prime bank scheme, perpetrators will offer investors the opportunity to buy notes, purportedly guaranteed by the world's top 100 banks, or "prime banks," which are fictitious financial instruments that allegedly offer high rates of return and safety.

was illegally copied. Information contained in the website—such as the company's name, address, and telephone numbers—were slightly altered or changed. The company CEO told us that the perpetrator who committed this scheme used the copied website to dupe foreign investors into sending funds to addresses listed. The company CEO also said that this scam went on for about 10 months, until the perpetrator moved on and copied another company's website and continued the scam.

Similarly, a Washington state securities official told us that a web site of a legitimate broker-dealer located in Seattle was copied and used to defraud foreign investors. The state official said that foreign investors were persuaded to purchase worthless stock certificates, and lost millions of dollars before the perpetrators decided to move on and copy another company's web site. Although the scam has not targeted U.S. investors, the regulator said that the securities division decided to pursue the case because it has the potential to undermine the reputation of and confidence in the U.S. securities markets.

SEC Has Established a Unit to Coordinate Efforts to Combat Internet Securities Fraud

SEC established the Office of Internet Enforcement (OIE) to coordinate the agency's response to increasing reports of Internet securities frauds.[6] OIE has several responsibilities, including developing policies and procedures for Internet surveillance, managing the E-mail complaint system, and providing guidance for conducting Internet securities fraud investigations. It has 3 full-time staff and about 125 volunteer staff in SEC headquarters and regional offices who work on a part-time basis to identify Internet fraud-related activities. Through its Office of Investor Education and Assistance, SEC has also established education programs to inform investors about the risks associated with Internet securities frauds.

OIE Established to Coordinate SEC's Internet Oversight Activities

In 1998, SEC established OIE to coordinate the agency's response to growing reports of Internet securities fraud. OIE's three full-time staff are responsible for a variety of oversight and coordination activities. For example, OIE has developed a policy manual to guide SEC's Internet surveillance activities. The manual provides guidance to SEC investigative staff on monitoring Internet web pages to identify potential securities frauds. OIE's Chief told us that the manual also includes guidance on conducting Internet securities fraud investigations. In addition, OIE provides training to staff from SEC, state regulatory agencies, and international regulators, and coordinates some of SEC's Internet securities fraud enforcement cases.

[6]Although SEC established OIE in 1998, OIE's Chief has been responsible for coordinating SEC's response to Internet frauds since 1995.

OIE also manages SEC's E-mail complaint system discussed earlier. OIE's Chief told us that staff review the E-mail complaints each day and decide the most appropriate action for each complaint. OIE's Chief also told us that some complaints are discarded because many complaints may refer to the same potential Internet securities fraud, in which case only a few complaints are retained; or because SEC already has an ongoing investigation into the alleged Internet securities fraud. According to OIE's Chief, staff refer other E-mail complaints—which the staff believe generally represent promising leads on potential securities frauds—to staff in SEC's enforcement division in headquarters or regional offices.[7] OIE may also refer complaints that do not involve violations of securities laws to other regulatory agencies, such as FTC. During calendar year 1998, OIE referred about 800 complaints[8] to other SEC units, and to other federal regulatory and enforcement agencies.

SEC's enforcement division and regional offices provide about 125 staff who work part-time on various Internet fraud-related activities. For example, SEC staff may volunteer to spend about 1 to 2 hours a week identifying potential securities frauds. Or, the SEC staff may work on Internet securities fraud investigations that were initiated on the basis of referrals made by OIE. SEC staff also may obtain information on potential Internet securities frauds from sources other than OIE. For example, senior officials in SEC's San Francisco district told us that enforcement actions had been initiated against alleged perpetrators of Internet securities frauds on the basis of information received directly from the public or through their own Internet investigations.

SEC Interagency Coordination Activities

OIE also has the responsibility to coordinate SEC's Internet oversight efforts with other federal regulators. OIE's Chief has met with officials in other organizations—such as NASD, NYSE, FTC, FBI, and the Secret Service—to discuss joint investigations pertaining to Internet fraud. As mentioned earlier, the OIE Chief said that OIE may refer E-mail complaints not related to violations of the securities laws to one of these organizations.

[7]OIE is also part of SEC's enforcement division.

[8]The potential exists that some of these complaints are not related to alleged Internet securities frauds. Based on our limited review of 100 complaints referred to SEC regional offices, and other federal regulatory and enforcement agencies, some of these referrals appear to relate to securities frauds, but do not involve the Internet. Other complaints appeared to be related to problems that customers have experienced with their broker-dealers. We did not systematically analyze these referrals to establish the percentage that were directly related to alleged Internet securities frauds.

In addition, OIE has coordinated SEC's participation in Internet "surf days," which are generally organized by FTC. On these assigned days, staff from a variety of organizations—including FTC, CFTC, SEC, NAASA, or foreign regulators—are to spend time surfing the Internet to identify potential fraudulent practices. In the November 1998 "Investment Opportunity Surf Day," agencies focused on identifying potential consumer financial frauds. The U.S. agencies that participated in the surf-day found dozens of cases among the over 400 web sites reviewed that potentially promoted consumer frauds. FTC officials told us that the regulators typically send warning messages to persons who operate such websites. Although the regulators do not ordinarily take enforcement actions on the basis of surf day findings, FTC officials said that the identified websites are monitored to determine if they are complying with the warnings. Failure to comply could result in enforcement actions.

SEC's Investor Education Programs

SEC's Office of Investor Education and Assistance has also developed education programs to inform investors about the risks associated with potential Internet securities frauds. According to its Director, SEC's primary message to individual investors is that investment decisions should not be based solely on information obtained over the Internet given the potential for fraud. Rather, the SEC official said that investors should perform a number of independent steps to ensure the accuracy of information provided about a stock over the Internet. These steps include reviewing financial information about the company that may be available from independent sources, determining whether the company is in fact developing a technology as advertised over the Internet, and contacting companies that are alleged to be in the process of signing contracts with the company in question. Unless investors are willing to take such steps, the SEC official said that investors may want to avoid using the Internet as a basis for making investment decisions.

SEC has implemented several programs to advise the investing public about the risks associated with the Internet and potential frauds. For example, SEC's website provides investor education information, such as procedures that investors should follow when assessing the reliability of on-line newsletters. SEC's webpage also contains information about the risks associated with Internet bulletin boards, chat rooms and mass E-mailings. In addition, SEC (1) produces pamphlets that discuss the risks associated with Internet securities investing; (2) holds local "town meetings" across the United States to discuss investment risks; and (3) coordinates the "Facts on Savings and Investing Campaign" with federal, state, and international securities regulators. This campaign is designed to educate individuals on saving and investing. The campaign released a

study in February 1998, entitled "The Facts on Savings and Investing," which, among other things, found that many Americans lack basic information about investing.

SEC Has Concluded About One-Half of the Internet Securities Fraud Cases Initiated Since 1995

SEC initiated a total of 66 judicial and administrative actions since 1995 to combat Internet securities fraud, and about one-half of these cases had largely been concluded[9] by February 1999. Because SEC is a civil rather than a criminal enforcement authority, SEC enforcement actions result in civil penalties---such as fines---rather than prison sentences for persons who are found to have violated securities laws. However, state or federal criminal enforcement authorities have also initiated criminal proceedings in 2 of these 66 cases, which have resulted in criminal convictions or prison sentences for 7 individuals.

SEC Has Statutory Authority to Pursue Civil Penalties

As provided by the Securities Enforcement Remedies and Penny Stock Reform Act of 1990 (the "Remedies Act"), SEC can seek civil money penalties in enforcement actions in federal district court or administrative proceedings against any individual or firm in the securities industry. The Remedies Act provides the district court with discretion in determining the civil penalty to be imposed in judicial proceedings. Depending upon the seriousness of the violation, SEC has the statutory authority to seek penalties that range from $5,500 to $1.1 million or up to 3 times the gross amount of the pecuniary gain to the defendant as a result of the violation.[10] Further, if the penalty is not paid within a prescribed time, SEC may request contempt proceedings in federal district court to compel payment.

According to SEC officials we contacted, the agency has limited staff and other investigative resources and is not able to pursue every credible allegation of securities law violations, including Internet frauds. Thus, SEC officials from the San Francisco district said that agency investigations often focus on message cases that have a high degree of public notoriety. According to the SEC officials, "message cases" are intended to punish wrongdoers for egregious offenses and deter other potential violations.

[9] We defined cases as "largely concluded" when a final judicial or administrative action was brought against at least one party in the case. These final actions include civil fines, disgorgements, permanent injunctions, cease and desist orders, prison sentences for defendants, and any combination thereof. Some of the cases that we define as largely concluded may have other litigation pending against one or more defendants.

[10] All penalties were increased to adjust for inflation as required by the Debt Collection Improvement Act of 1996. The increase was effective December 9, 1996.

One-Half of All SEC Enforcement Actions Have Been Concluded

As of February 1999, a penalty or injunctive order had been imposed on at least one of the defendants in 32 of the 66 Internet securities fraud cases SEC initiated since 1995. Litigation was pending in the other 34 cases. In 21 of the 32 cases that have largely been concluded, violators were required to pay some form of civil money penalty. Specifically, violators were required to (1) pay civil fines, (2) disgorge illegally obtained profits to compensate defrauded investors, or (3) pay both civil fines and disgorgements. The civil fines that SEC imposed ranged from $5,000 to $4.4 million, while the disgorgements ranged from $500 to $4.4 million.

In nine other cases that have largely been concluded, a civil money penalty was not imposed on the violators. Instead, SEC primarily obtained a cease and desist order or permanent injunction to prevent further violations of the securities laws. In the remaining two cases, prison sentences or other criminal convictions were imposed by a state or federal court. According to DOJ officials we contacted, the department or the FBI would become involved in Internet securities fraud cases where there are widespread losses and many victims.

Many States Also Reported Implementing Programs to Control Internet Securities Fraud

We also obtained survey information from the 50 state securities regulatory agencies about state efforts to control Internet securities fraud and penalize state securities law violators.[11] Nearly one-half of the state agencies reported that they have implemented specific Internet securities fraud control programs over the past several years—such as surfing the Internet to detect potential frauds. Many states have also initiated enforcement actions to penalize individuals who use the Internet to violate state securities laws. However, some state agency officials report that state enforcement actions are not always effective because perpetrators prohibited from selling securities in one state can continue to sell securities in other states.

Nearly One-Half of All the States Have Implemented Programs To Combat Internet Securities Fraud

In 23 of the 50 states we surveyed, officials from regulatory agencies reported establishing specific programs to control Internet securities fraud and penalize violators of state securities laws. In 14 of these 23 state regulatory agencies, the programs generally consisted of one or more persons surfing the Internet using word searches, such as “investment,” “finance,” or the name of their state to detect fraudulent activity. Other states reported monitoring Internet bulletin boards, newsgroups, and chat

[11]We conducted a structured telephone survey of securities regulatory agencies in all 50 states from December 1998 through January 1999. We asked primarily the Directors of these agencies, among other things, to describe whether or not their agencies had established specific programs to combat Internet fraud and the types of penalties imposed on violators. We obtained data about New York from an official of the New York Attorney General’s Office.

rooms to identify potential securities frauds. The frequency at which these states reported conducting Internet monitoring varied widely among the states, ranging from one-half hour daily to 2 hours weekly to one time per month.

Regulatory officials from the other 27 state agencies that we contacted said they had not established specific programs to identify and combat Internet securities fraud. The officials cited several reasons for not establishing specific programs, such as inadequate technical expertise or, as in two cases, a lack of Internet access. In addition, officials from some of the other smaller state agencies said that the control of securities fraud on the Internet was the responsibility of the federal government and that their agencies would not be in a position in terms of available resources to handle the problem.

Applicability of State Enforcement Actions May Be Limited

Officials from 31 of the 50 states we surveyed said that their regulatory agencies had initiated a total of about 190 enforcement actions against persons and companies accused of violating state securities laws through the use of the Internet. The number of enforcement actions initiated per state ranged from 1 to 22. The remaining 19 states had not initiated any enforcement actions related to Internet securities fraud.

Based on the results of our survey, states that have implemented specific Internet fraud securities control programs collectively initiated about three times as many enforcement actions as the states that did not have a program in place. About 146 enforcement actions were initiated across the 23 states that implemented programs compared with about a total of 48 actions that were filed across the 27 states that did not establish a program.[12] Nearly all of the enforcement actions initiated by the states resulted in warning letters, informal agreements, or the issuance of cease and desist orders. However, as discussed previously, state criminal enforcement authorities have pursued criminal cases as well.

An enforcement action brought by one state may deter persons or companies from committing fraudulent acts in that state, but it does not necessarily prevent persons or companies from committing the same scam through the Internet in other states. For example, a Pennsylvania securities official reported that the state took an administrative action against a company that disseminated Internet spam that called for investors to purchase interests in a trust and realize an 80 to 160 percent

[12]Other factors, such as the size of the state's securities staff and the number of frauds originating from a particular state can also account for this difference.

return on their investment. Although the administrative action prohibited the company from selling these interests to Pennsylvania residents, the company reportedly defrauded about 1,500 residents in other states who bought about $3 million in interests.

Moreover, California securities enforcement officials reported that if enforcement actions are initiated against companies located overseas, these companies tend to ignore the orders and continue to sell their securities. For example, the enforcement officials told us that an order was issued to a company located in England to stop the offer and sale of securities and convertible bonds in time travel ventures in the state of California. However, the officials said that the British company continued to fraudulently sell securities and bonds over the Internet, including to California residents.

Regulatory Challenges in Combating Internet Securities Fraud

Although SEC and state regulatory agencies have initiated programs to combat Internet securities frauds, these programs are new, and it is too early to predict their long-term effectiveness. On the basis of our work, we identified several potential challenges that could limit the ability of these programs to protect investors from Internet scams. In particular, the potential exists that the rapid growth in reported Internet securities frauds could ultimately place a significant burden on the regulators' limited investigative staff resources and thereby limit the agencies' ability to respond effectively to credible fraud allegations. Another ongoing challenge is coordinating oversight among international, federal, and state securities regulators so that fraudulent operators are deterred from taking advantage of the fact that Internet frauds can be initiated from virtually anywhere in the world. A final challenge involves educating the investing public about the risks associated with Internet securities frauds. Since regulatory resources are limited, preventing investors from falling for Internet securities frauds in the first place may be the best way to contain the problem.

The Rapid Growth of Reported Internet Securities Frauds Poses Challenges to Limited Regulatory Investigative Resources

The rapid expansion of the Internet and the growth of securities-related activities over the past several years pose potential challenges to SEC and state regulatory agencies to control securities fraud on the Internet. According to SEC's OIE Chief, the rapid expansion in E-mail complaints from 10 to 15 daily in 1996 to 200 to 300 complaints daily in early 1999 suggests that the agency may ultimately reach a point where it cannot respond to all credible allegations of Internet securities fraud. Given its present staffing levels, SEC officials said that the agency already tends to focus investigations on certain high-profile cases, including Internet fraud cases. We also note that over the past several years a significant number

of SEC attorneys who are responsible for investigating Internet and other securities fraud cases have left the agency for higher-paying jobs in the private sector. For example, SEC reports that between 1996 and 1998 SEC's New York office lost 54 percent of its 137 enforcement staff and the San Francisco office lost about 40 percent of its 25 enforcement staff.

State regulatory officials we contacted said that their agencies have few staff allocated to investigate Internet fraud cases. For example, many state officials said that their agencies have no more than five staff to investigate and enforce all relevant state securities laws, so finding the time to adequately monitor the Internet to detect potential frauds can be difficult. Further, officials from some other state agencies said that specific programs to monitor Internet fraud have not been established in their organizations due to limited staff.

Given that the Internet has millions of web-sites[13] and the regulators' belief that a large number of these sites, on-line newsletters and spams include schemes intended to defraud investors, SEC and state regulators may also face challenges in obtaining the technical capacity to comprehensively monitor the Internet and detect potential securities frauds. According to state regulatory officials, their staff mainly surf the Internet using commercial search engines and key word searches to detect potential frauds, which is a method that an official from the National White Collar Crime Center said is labor intensive and inherently inefficient. The official also said regulators should develop customized search engines to detect potential Internet frauds that could relieve staff of the labor-intensive search activities and thereby enhance regulatory efficiency. SEC's OIE Chief told us that use of customized search engines can help facilitate the detection of Internet securities frauds, but such devices are no substitute for the judgement of experienced, investigative staff trained in methods to identify potentially fraudulent activities. Further, the OIE Chief said that developing such customized search engines could place demands on a regulator's limited financial resources.

[13]Latest estimates show that as of July 1998, the Internet consisted of about 37 million web sites. Source: Internet Domain Survey, July 1998, Network Wizards http://www.nw.com.

Regulators Face Challenges in Maintaining a Coordinated Approach to Combating Internet Securities Fraud

The global nature of the Internet increases the regulatory challenges of combating Internet securities fraud because the Internet for the most part does not recognize jurisdictional boundaries. Now, a fraudulent operator from anywhere in the world could solicit U.S. investors linked to the Internet. Even in the United States, fraudulent operators located in one state can use the Internet to defraud residents of other states, even though another state has taken action directing the operator to cease and desist. Jurisdictional issues are challenging because close coordination and cooperation among international, federal, and state securities regulators is required to prosecute violators and hopefully, deter additional Internet frauds.

The regulatory challenges associated with investigating overseas Internet securities fraud cases include obtaining evidence, convincing other governments to prosecute foreign entities and individuals, and ensuring restitution for victims. A 1997 report[14] by the International Organization of Securities Commissions (IOSCO),[15] argued that securities regulators need to establish well-defined mechanisms for cooperating with their foreign counterparts to respond to these challenges and deter Internet frauds. For example, IOSCO recommended that securities regulators develop policies and procedures to ensure the timely exchange of information about ongoing investigations of Internet securities fraud. IOSCO also stated that coordination should include sharing information about (1) Internet surveillance techniques, (2) questionable transactions that may represent potential Internet frauds, and (3) successful approaches to prosecuting Internet securities fraud cases.

State securities regulatory agencies face similar challenges in developing a coordinated approach to Internet fraud investigations and enforcement. As pointed out earlier, state enforcement actions may have limited success because Internet securities frauds may be committed from out-of-state locations. Challenges facing states include working with other regulatory agencies to combat fraudulent schemes that operate across states, ensuring sufficient monitoring of the Internet by other jurisdictions, and obtaining necessary evidence to initiate enforcement action.

[14]Report on Enforcement Issues Raised by the Increasing Use of Electronic Networks in the Securities and Futures Field. IOSCO (September 1997).

[15]IOSCO is an international organization of securities regulators—including SEC—whose mission is to promote global coordination in the regulation of the securities industry.

Regulators Face Challenges in Educating the Investing Public on the Risks Associated with Internet Securities Frauds

According to SEC, investor education is a critical defense against Internet securities frauds given the fact that regulatory resources to combat the problem are limited. If investors are adequately informed about the risks associated with potential Internet securities frauds, then they will be less likely to fall victim to sophisticated scams. The investor education challenges facing regulatory agencies include identifying schemes or mechanisms that require further investor awareness and widely disseminating information about the risks associated with Internet in a timely and effective manner. While SEC has taken steps to educate the public that investment decisions should not be made solely on the basis of information received over the Internet, ensuring that such warnings reach a wide audience is a difficult challenge. SEC's investor education initiatives to date—such as posting information on the SEC website and producing pamphlets—are relatively low cost and have a limited ability to reach a wide audience. For example, not all investors may be aware that SEC has posted investor education information on its website. Reaching a large audience with relevant investor information often involves conducting large media campaigns that could be expensive and may take a long time to produce results. SEC's capacity to educate investors and disseminate widely relevant information about the potential risks of Internet securities frauds may be limited. According to SEC, the agency's budget and staff resources directed to investor education have remained relatively stable over the past several years, so the agency's capacity to initiate large-scale media campaigns is limited.

In summary, Ms. Chairman we commend you for holding this hearing and thank you for inviting us to testify on our preliminary observations on Internet securities fraud and regulatory efforts to combat this growing problem. Hearings such as this are particularly useful because they provide a public forum for educating large numbers of investors that while the Internet has much to offer, there are potential risks as well. We look forward to working with you and your staffs in this important area.

Ms. Chairman, this concludes my prepared statement. My colleague and I would be pleased to answer any questions that you or Members of the Subcommittee may have.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Order by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touch-tone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested