Creative Sanctions for Online Investment Fraud

Jayne W. Barnard

William & Mary Law School, jwbarn@wm.edu

Copyright © 2007 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.

https://scholarship.law.wm.edu/facpubs/135
CREATIVE SANCTIONS FOR ONLINE INVESTMENT FRAUD

Jayne W. Barnard

As long as promoters have sought to raise money for their ventures, fraud has been a feature of the marketplace.¹ Throughout commercial history, some stock promoters have touted their product, misrepresented its value, and manipulated its pricing. Eager investors have often parted with their money impulsively, overpaid for worthless or near worthless stock, and later complained that they were misled.

This Article will examine the current environment in which stock promoters sell their wares. Increasingly, stock scams are not confined to face-to-face encounters or multi-telephone-line, high-testosterone “boiler rooms.” Rather, investment fraud—like other forms of fraud—is migrating to the Internet. According to the National White Collar Crime Center, online investment fraud is now the fifth most common form of Internet fraud.² Since its creation in 1998, the SEC’s Office of Internet Enforcement has handled cases involving hundreds of millions of dollars in investor losses.³

¹ The Roman playwright Plautus describes the “puffers” and the “impudent, talkative, and malevolent fellows” who populated the Roman Forum in the second century B.C. EDWARD CHANCELLOR, DEVIL TAKE THE HINDMOST: A HISTORY OF FINANCIAL SPECULATION 4 (2000).


³ See, e.g., Andrew Leckey, Fraud Dresses Up On Web, But It’s Still Crime, CHI. TRIB., Apr. 2, 2006 at C6 (noting that, since 1998, the office has handled
Part I of this Article will briefly examine the current patterns of securities fraud schemes, especially those schemes that depend on the use of the Internet (including e-mail) for successful execution.

Online investment fraud is usually the subject of civil enforcement, both at the state and federal level, not criminal prosecution. Still, some securities fraud schemes—and particularly some Internet-based securities fraud schemes—warrant criminal prosecution. Part II of this Article will explore the current tools available to sanction securities law violators. Under federal law, several sentence enhancements are available that seem particularly applicable to online investment schemes; state law, too, provides some guidance on the appropriate sentence for securities law violators.

Current federal law, however, has some holes in it as regards online fraud schemes, including online investment schemes. In Part III of this Article, I will sketch out three possible amendments to the Federal Sentencing Guidelines that would improve the sentencing regime available for perpetrators of online investment fraud. I will also encourage the creation of a securities fraud registry—modeled after sex offender registries—to assist potential investors in knowing with whom they are dealing.

I. TODAY’s ELECTRONIC INVESTMENT SCHEMES

Historically, many securities frauds involved face-to-face encounters in which an aggressive salesman promoted (or “touted”) an overvalued security.4 In the 1960s, so-called “boiler rooms” emerged, in which a battery of high-pressure salesmen worked from phone banks, making cold calls to customers’ offices and homes and soliciting the purchase of securities—often thinly-traded stocks known as “penny stocks.”

nearly 600 Internet-related cases).


Today, more and more investors are seeking investment opportunities on the Internet. Their comfort level in doing so traces to four factors: (1) many of these investors experimented with day trading during the 1990s and became accustomed to the process of identifying and purchasing stocks online; (2) search technologies such as Google have made the search for investment opportunities cheap and easy; (3) issuer websites, investor message boards, and chat rooms have streamlined the process of gathering information about companies and their prospects—both reliable and unreliable information; and (4) payment systems such as PayPal and the routine use of credit cards online have made the entire process of buying securities as easy as buying a pair of shoes.

There is also a seductive aspect of searching for investment opportunities online. Somehow, a person who goes looking for investment information and comes up with something she thinks is an attractive opportunity feels more empowered and confident than had she received a cold call from a salesman. One assumes that a securities salesman has a strong interest in making a sale and may over-promote the product, but somehow visiting a website that facilitates a securities purchase seems more objective—and safer—than making a decision in response to an obvious solicitation. In fact, it often feels as if no solicitation has taken place at all but rather the investor has made her own, exciting discovery.

Investor message boards have played a special role in building investors’ confidence in today’s markets. Even though most investors presumably understand that message boards can be manipulated by posters harboring a hidden agenda, they still may attribute to bulletin board posts a sense of real-

ity they would not attribute to a sales call. That is, reading dozens of posts about a company may reassure the reader that she has captured the insights of others with no axe to grind, confirm that others have made the same decision (to buy or sell) being contemplated by the reader, and persuade her that she has the benefit of some kind of insider information. As one experienced investor recently revealed in a memoir about the HealthSouth fraud case, “I was convinced that message boards provide valuable access to investment information available nowhere else.”

These developments—and investors’ increasing comfort level with making investment decisions unaided and online—inevitably have fostered a growing online fraud industry.

What do these online stock frauds look like? Not surprisingly, they often look much like yesterday’s fraud schemes, just slicker. Thus, we find issuers selling securities from corporate websites that misrepresent their assets, revenues, and realistic prospects for the future; issuers purporting to sell securities then absconding with the proceeds of the offering;

---


7 See, e.g., SEC v. Inv. Tech., Inc., Litigation Release No. 18970, 2004 SEC LEXIS 2624 (Nov. 15, 2004), available at http://www.sec.gov/litigation/litreleases/ltirelarchive/ltirelarchive2004.shtml (describing promoter’s claims that an Internet-based gambling site had already handled $4 million in wagers, when in fact the company had no history of operations or revenue); SEC v. Toks, Inc., Litigation Release No. 18309, 2003 SEC LEXIS 2040 (Aug. 25, 2003), available at http://www.sec.gov/litigation/litreleases/ltirelarchive/ltirelarchive2003.shtml (describing issuer’s claims it intended to launch tender offers for several major public companies, when in fact it had no revenue or assets and only one employee, so it “had no ability to conduct the contemplated tender offers”).

issuers selling unregistered securities from their websites; issuers selling interests in "Ponzi schemes" or "pyramid" schemes; issuers promoting so-called "risk-free" investments when in fact the investments are risky or even fictitious; and issuers engaged in a modern version of the "pump-and-dump" or stock price manipulation scheme. Some of the schemes are surprisingly simple—"outing" violations, for example, where the promoter fails to disclose that he is being compensated for his role in the offering, or where the issuer


13 See infra notes 16-28 and accompanying text.

falsely claims that its products are FDA-approved.\textsuperscript{15}

Some online stock frauds, however, depend on the unique features of the Internet for their success and represent more than just a high-tech version of age-old techniques. Here are some examples.

In one scheme that gained notoriety on the news program \textit{60 Minutes}, a high school student named Jonathan Lebed engaged in a fairly simple pump-and-dump scheme using the Internet.\textsuperscript{16} First he purchased large blocks of shares in thinly-traded microcap companies, using his father's trading account.\textsuperscript{17} Then, using multiple identities and usernames, Lebed made thousands of posts onto Yahoo's investor message boards, offering statements like "[this stock is] about to take off," "[it will be] the next stock to gain 1000%," and "[this] is the most undervalued stock ever."\textsuperscript{18} By creating the appearance of intense enthusiasm across a large number of investors, Lebed was able to sell his shares at the top of the market, and profited by at least $272,000.\textsuperscript{19}

In another scheme, another high school student, Benjamin Snyder, held stock in Viragen International, Inc., and wanted to sell his stock at a profit.\textsuperscript{20} He not only posted false statements on investor message boards, but also created a phony news story that looked like it had come from the Bloomberg news service.\textsuperscript{21} He used the name of an actual Bloomberg re-


\textsuperscript{17} Id.

\textsuperscript{18} Id.

\textsuperscript{19} Id.


\textsuperscript{21} Id.
porter as the purported source of the news story. People reading about Viragen on the message boards often clicked through to the phony Bloomberg news story, and were persuaded on that basis to buy—and drive up the price of—the stock.

Yet a third Internet scheme involved law students at Georgetown Law School. The students created a website—“Fast-Trades.com”—on which they offered stock recommendations. They promoted their website by posting hundreds of messages on investor message boards. “These messages disguised the authors’ connection with the site and misrepresented the investment success they achieved from following Fast-Trades’ recommendations.” The students relied on a growing subscriber base at Fast-Trades.com to buy stock on the basis of the website’s recommendations, thus driving up the stock price, whereupon the students would sell their pre-purchased shares. The students netted more than $345,000 on the scheme.

Other pump-and-dump schemes involved the creation of—and links to—phony “analysts’ reports,” the creation of a “Red Hot Stocks” website to promote the defendants’ companies and their stocks, and the distribution of “spam” e-mail

22 Id.
23 Id.
25 Id.
26 Id.
27 Id.
28 Id.
messages endorsing the defendants' specified companies.\textsuperscript{31}

Recently, some new forms of online investment frauds have emerged and these, too, are dependent on the special features of the Internet. In one scheme, the promoters created a "virtual stock exchange" on which—for a fee—people could trade in "virtual stock."\textsuperscript{32} Through computer programming, the price of the virtual stock would rise and fall.\textsuperscript{33} The promoters promised a minimum gain on each "virtual" investment of 10% per month (or 215% a year).\textsuperscript{34} In fact, the scheme was an old-fashioned Ponzi scheme, in which later-arriving investors would fund the payoffs to earlier-arriving investors.\textsuperscript{35} The scheme netted more than $5 million before it was interrupted by the SEC.\textsuperscript{36}

Another scheme that depends on the Internet is the stock-related "cybersmear." Here, short-sellers drive down the price of a stock by posting negative, false information on investor message boards.\textsuperscript{37}

Yet another Internet-dependent scheme is the recently-dismantled "auto-surfing" scheme.\textsuperscript{38} Here, the promoter induced victims to participate in a program in which they were promised payment merely for "clicking and looking" at certain web pages.\textsuperscript{39} The premise behind the scheme was that com-

\begin{footnotesize}
\begin{enumerate}
\item [33] Id.
\item [34] Id.
\item [35] Id.
\item [36] Id.
\item [39] Id.
\end{enumerate}
\end{footnotesize}
panies that advertise on the Internet are willing to pay to increase traffic to their web sites. These companies hire an auto-surf firm or "host," which in turn pays individual web surfers to view certain web sites on an automatically rotating basis. The more sites the individual visits, the more money he or she stands to earn.

The problem with this scheme was that, once a victim was "hooked" with small payments for "clicking and looking," there was a charge to continue in the program. Victims were asked to purchase "membership units," which would entitle them to additional "clicks" each day. The scheme, however, was really a Ponzi scheme. Before being shut down, the website was ranked as the 352nd most heavily-trafficked web site in the United States. The scheme is said to have raised more than $50 million from over 300,000 investors worldwide.

Two final Internet-based securities fraud schemes do not, in fact, involve securities fraud at all, in any conventional sense. In the first case, the defendant hacked into an online trading account and electronically caused an unknown victim to "purchase" soon-to-be-worthless stock options owned by the defendant. The defendant thereby avoided $37,000 in foreseeable losses. Because the victim did not in fact make any investment decision, but was an unwitting buyer, this scheme does not seem to fit the traditional pattern of inducing a purchase based on a material misstatement or omission. The second case involved the giveaway of "free stock" in order to create the appearance of an active market, with recipients

40 Id.
41 Id.
42 Id.
43 Id.
44 Id.
45 Id.
46 Id.
48 Id.
induced to sign up for the offer with gross overstatements of the “free” stock’s value. Here, too, the victims did not make investment decisions—they merely accepted gifts of (usually worthless) stock.

II. THE EXISTING TOOLKIT

Since 1934, securities law violations have been subject to a civil enforcement regime presided over by the Securities and Exchange Commission (SEC). Over that period, the SEC has acquired a wide range of enforcement tools, which today includes the authority to seek a court-ordered asset freeze, to enter and enforce its own cease-and-desist orders against wrongdoers; to suspend or bar regulated professionals from continuing to serve in their professional roles; to seek a “penny stock bar,” an “officer and director bar,” injunct-

50 Id.
51 See, e.g., SEC v. Tanner, Litigation Release No. 19325, 2005 SEC LEXIS 1990 (Aug. 4, 2005), available at http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (involving the interruption of the sale of so-called “high yield” bonds, in which the proceeds of the offering—more than $15 million—were sent offshore; the court entered an asset freeze against the issuer, individual defendants, and one defendant’s mother).
tive relief, the imposition of civil penalties, the appointment of a court-appointed receiver, and disgorgement of profits to compensate victims.

This Article, however, is about what happens when the SEC cedes its authority to the Department of Justice to pursue criminal sanctions against a defendant. Specifically, this Article considers some of the ways in which federal prosecutors might deal with online investment frauds in the criminal context.

Under the Federal Sentencing Guidelines (Guidelines), prosecutors necessarily must deal with both the “offense level” of the crime (based upon the amount of loss occasioned by the

---


fraud)\(^{60}\) and the criminal history of the defendant (through which recidivists get appropriate credit for their criminal histories). Beyond these foundational items, however, there are provisions in the Guidelines for sentence enhancements that seem particularly well-suited to the circumstances of many online investment frauds. These provisions authorize sentence enhancements for the use of “mass-marketing,” the involvement of multiple victims, the use of “sophisticated means” in perpetrating the crime, the use of “special skills,” relocation from state-to-state or out of the United States in order to thwart detection of the crime, and significant use of offshore resources.\(^{61}\) Sentence enhancements are also possible for the organizers or leaders of “extensive” fraud schemes.\(^{62}\) And there is always the possibility of an upward departure to take into account aggravating factors not otherwise dealt with within the Guidelines.\(^{63}\) Prosecutors also may seek restrictions on Internet access for defendants as a condition of probation or supervised release.\(^{64}\)

A. Use of “Mass-Marketing”

The Federal Sentencing Guidelines provide for a two-level sentence enhancement where the crime “was committed through mass-marketing.”\(^{65}\) “Mass-marketing” is defined as “a plan, program, promotion, or campaign that is conducted through solicitation by telephone, mail, the Internet, or other means to induce a large number of persons to (i) purchase goods or services; (ii) participate in a contest or sweepstakes; or (iii) invest for financial profit.”\(^{66}\)

There should be little question that the “mass-marketing” enhancement should apply to online securities frauds conducted over the Internet, just as it does to non-securities related

\(^{60}\) U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b).

\(^{61}\) See infra, Sections A, B, C, D, E, and F.

\(^{62}\) See infra, Section G.

\(^{63}\) See infra, Section H.

\(^{64}\) See infra, Section I.


\(^{66}\) U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. 4(A).
frauds conducted over the Internet.67

B. High-Volume Victimization

The Sentencing Guidelines provide for a two-level sentence enhancement where the fraud involves ten or more victims.68 Courts are authorized to enter a four-level enhancement where the fraud involves fifty or more victims.69 Frauds involving 250 or more victims can result in a six-level enhancement.70 These enhancements can easily be applied to widespread online securities frauds.71

C. "Sophisticated Means"

The Federal Sentencing Guidelines provide for a two-level sentence enhancement where the defendant’s crime involved “sophisticated means.”72 To date, judges in reported federal court opinions have not found that the use of an interactive website itself constitutes “sophisticated means.”73 Reasoning by analogy, however, use of a website (or websites) in an online investment fraud should constitute “sophisticated

---

67 See, e.g., United States v. Nickens, 38 F. App’x 721 (3d Cir. 2002) (affirming a two-level “mass-marketing” enhancement where defendant conducted an auction scam over the Internet); United States v. Blanchett, 41 F. App’x 181 (10th Cir. 2002) (holding the same); United States v. Pirello, 255 F.3d 728 (9th Cir. 2001) (affirming a two-level “mass-marketing” enhancement where defendant pleaded guilty to wire fraud in connection with the fraudulent sale of computer equipment over the Internet).


70 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(2)(C).


72 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(9)(C). "For purposes of subsection (b)(9)(C), ‘sophisticated means’ means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense. For example, in a telemarketing scheme, locating the main office of the scheme in one jurisdiction but locating soliciting operations in another jurisdiction ordinarily indicates sophisticated means." Id. cmt. n.8.

73 See, e.g., United States v. Clark, 2004 FED App. 03-5624 (6th Cir.), 117 F. App’x 430. The opinion indicates that the United States Probation Office regards the use of a website alone as constituting a “sophisticated means.” Id. at *432.
if the creation of a website is now very simple.

We know, for example, that the use of the Internet for communication and transmission of images, together with the use of a webcam, satisfies the "planning [and] sophistication" aggravating factor under California law.\textsuperscript{74} So does the extraction of money from victims "by means of the Internet and the use of false identities."\textsuperscript{75}

Certainly, an elaborate identity theft scheme in which the defendant gathers personal information on the Internet, and then, using that information, makes purchases in his victims' names by telephone, satisfies the "sophisticated means" requirement of federal law.\textsuperscript{76}

I would argue that online investment frauds that use multiple websites, especially those involving purported links to phony analysts' reports and press releases, or posts purporting to come from multiple sources (and using multiple usernames) should satisfy the "sophisticated means" requirement. Just because the creation of a website (or multiple websites) is easy—many teenagers do it, and there are "build-a-website" instructions all over the Internet today\textsuperscript{77}—does not negate the fact that many online investment schemes require the creation and maintenance of a complex set of sites and identities.

Certainly a Ponzi scheme, in which early investors are paid with the revenue received from investors arriving later, itself requires "sophisticated means," even where it does not involve the use of the Internet.\textsuperscript{78}

\textsuperscript{76} United States v. Jackson, 346 F.3d 22 (2d Cir. 2003).
\textsuperscript{78} United States v. Bistrup, 449 F.3d 873 (8th Cir. 2006).
D. Use of a "Special Skill"

The Federal Sentencing Guidelines authorize the imposition of a two-level enhancement where the defendant "used a special skill, in a manner that significantly facilitated the commission or concealment of the offense."\(^7\) A "special skill" is defined as "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing."\(^8\)

Many courts agree that a defendant need not have had a formal education to qualify for a special skill enhancement.\(^8\) Thus, a self-taught hacker who used his computer skills to retrieve personal data from the Internet in an identity-theft scheme was given a two-level "special skills" enhancement.\(^8\) A disgruntled ex-employee who used his knowledge of his employer's computer system to enter the site and destroy valuable data was given a two-level sentence enhancement because he had skills "beyond those possessed by an ordinary computer user."\(^8\) The Court of Appeals said nothing about whether his scheme required formal education.

Some courts, however, are reluctant to impose a "special skill" enhancement on defendants who used their computer skills to engage in online fraud, primarily because those skills do not require formal education. Thus, a clever programmer who created a "mirror" website for the Honolulu Marathon in Japanese, rather than English, and who then misappropriated registration fees from Japanese runners, was found ineligible for a "special skills" enhancement because his computer skills were not "particularly sophisticated."\(^8\) Likewise, a defendant who used his computer skills to produce counterfeit bills on

---

\(^7\) U.S. SENTENCING GUIDELINES MANUAL § 3B1.3 (2005).
\(^8\) Id. cmt. n.4.
\(^9\) United States v. Prochner, 417 F.3d 54, 61 (1st Cir. 2005).
\(^10\) Id. at 62; see also United States v. Petersen, 98 F.3d 502 (9th Cir. 1996) (hacker given a two-level enhancement, although he had had no formal training on computers).
\(^11\) United States v. O'Brien, 435 F.3d 36, 42 (1st Cir. 2006).
\(^12\) United States v. Lee, 296 F.3d 792 (9th Cir. 2002) (overturning enhancement).
Adobe Page Maker was also found not to be eligible for a “special skills” enhancement.85

It would be useful, of course, to have a little more guidance from the courts on just how much “sophistication” is required of computer-based schemes for the “special skills” enhancement to be appropriate. We do know, however, that the “sophisticated means” enhancement and the “special skills” enhancement are not identical (and, therefore, are not mutually exclusive).86 So the question of “sophistication” may not really be the right one to ask on the issue of whether the defendant employed special skills. Rather, the question should be whether an “ordinary” computer user would be able to fashion the type of website or interactive program necessary to execute a particular securities fraud scheme.

E. Relocating to Avoid Detection

The Federal Sentencing Guidelines authorize the trial courts to impose a two-level sentence enhancement where the defendant “relocated, or participated in relocating, a fraudulent scheme to another jurisdiction to evade law enforcement or regulatory officials.”87 This provision encompasses a defendant’s relocation from state to state, as well as relocation outside of the United States.88 Many securities law violators have a history of moving from state to state and taking their schemes with them. A relocation enhancement might well be appropriate for defendants in this category. One might also argue that a securities law violator that moves from website to website or from server to server should also be eligible for a “relocation” enhancement.

86 United States v. Olis, 429 F.3d 540, 549 (5th Cir. 2005); United States v. Minneman, 143 F.3d 274, 283 (7th Cir. 1998) (“The special skill adjustment focuses on [the defendant’s] use of his [professional] training. The sophisticated means enhancer arises because of the use of multiple accounts and corporate names. Thus, both enhancements could be invoked.”).
88 United States v. Stokes, 75 F. App’x 888 (3d Cir. 2003).
F. Use of an Offshore Location

The Federal Sentencing Guidelines authorize the trial court to impose a two-level sentence enhancement where "a substantial part of a fraudulent scheme was committed from outside the United States." Many securities fraud schemes are now orchestrated from outside the United States, raising significant enforcement problems. To the extent that the government is able to bring the perpetrators of these schemes to justice in the United States, this two-level enhancement is custom-built just for them.

G. Aggravating Role

The Federal Sentencing Guidelines authorize the imposition of a three- or four-level enhancement where the scheme involves five or more participants, and the defendant served as the "organizer or leader," or "manager or supervisor" of the scheme. An "organizer or leader" is more culpable than a "manager or supervisor" and thus is subject to an extra one-level enhancement. This set of enhancements also takes into account the existence of unwitting accomplices.

These provisions will have no application to a con artist who single-handedly, creates a website and handles all of the postings and communications involved in executing an online investment scheme. However, schemes involving five or more actors invite the application of one of these "role" enhancements.

---

92 Id. cmt. n.3 (construing the term "otherwise extensive" as including unknowing outsiders).
93 See, e.g., United States v. Aptt, 354 F.3d 1269, 1285 (10th Cir. 2004) (affirming a four-level "organizer or leader" enhancement for a defendant who orchestrated a Ponzi scheme).
H. Upward Departures for Crimes "Outside the Heartland"

The Federal Sentencing Guidelines provide for departures from the calculated sentence where the court finds "an aggravating or mitigating circumstance... not adequately taken into consideration by the Sentencing Commission in formulating the guidelines."94 Departures are typically applied to sentences imposed for crimes that are said to be "outside the heartland" of the "typical" crimes around which the Sentencing Guidelines were formulated.95

An upward departure in a fraud case may be appropriate where the defendant is a recidivist, his misconduct extends over a period of years and across several states, and reaches victims all over the United States.96 It may also be appropriate where the scheme is extensive both in terms of the amount of money extracted and the number of victims ensnared, especially where the result is that "thousands of investors lost their life savings."97 Courts may focus on the fact that victims have lost "irreplaceable" funds and have been unable to meet their financial obligations.98

I. Limitations on Access to the Internet as a Condition for Probation or Supervised Release

There is one final tool available to prosecutors, in addition to sentence enhancements and upward departures. Federal and state courts often impose conditions on a sentence of probation or supervised release, including limitations on computer or Internet usage. While a complete ban on Internet access may be appropriate in some cases (typically involving defendants convicted of the online sale of child pornography),99

---

96 United States v. Passmore, 984 F.2d 933, 938 (8th Cir. 1993) (affirming upward departure).
97 United States v. Stouffer, 986 F.2d 916, 928 (5th Cir. 1993) (affirming upward departure).
98 United States v. Scrivener, 189 F.3d 944, 951 (9th Cir. 1999) (affirming a two-level upward departure).
99 See, e.g., United States v. Fields, 324 F.3d 1025, 1027 (8th Cir. 2003).
limitations on access must be reasonably related to the defendant’s rehabilitation and protection of the public.\textsuperscript{100}

Within this boundary, federal courts have limited Internet access in a number of specific ways. For example, one defendant with a history of identity theft was permitted to use the Internet at work, “so long as he ha[d] no access to personal information including bank account numbers, credit card numbers, social security numbers and birth dates.”\textsuperscript{101} Another defendant was prohibited from accessing any Internet bulletin boards unless specifically approved by the U.S. Probation Office.\textsuperscript{102}

Defendants permitted some access to computers may, as a condition of supervised release, be denied access to certain types of hardware or software consistent with their criminal history.\textsuperscript{103} Their access to a computer may also be conditioned upon installation of a monitoring application, such as a keystroke-reading program, and subject to random monitoring by the U.S. Probation Office.\textsuperscript{104}

State courts have also imposed restrictions on access to the Internet in some cases. These kinds of restrictions are common for sex offenders whose crimes involved Internet com-

\textsuperscript{100} See United States v. Crume, 422 F.3d 728, 732 (8th Cir. 2005) (articulating the limitations that govern conditions of probation or supervised release); United States v. Scott, 316 F.3d 733, 735 (7th Cir. 2003) (cautioning against too aggressive use of restrictions on Internet access as a condition of probation or supervised release).

\textsuperscript{101} United States v. Stanfield, 360 F.3d 1346, 1352 (D.C. Cir. 2004) (remanding case for clarification of the scope of the restriction).

\textsuperscript{102} United States v. Crandon, 173 F.3d 122, 128 (3rd Cir. 1999).

\textsuperscript{103} See, e.g., United States v. Goba, 220 F. Supp. 2d 182 (W.D.N.Y. 2002). The defendant was not allowed to possess, purchase, or use a computer that included a modem, Internet account, writable or rewritable CD Rom, tape backup or removable mass storage device. Id. at 195. “If allowed use of a computer for employment, the system [could] only contain software required to perform his job.” Id. at 196.

\textsuperscript{104} See, e.g., United States v. Liu, No. 03 Cr. 782 (LTS), 2006 U.S. Dist. LEXIS 13849, at *3-16 (S.D.N.Y. Mar. 29, 2006) (detailing the conditions imposed on the defendant by the U.S. Probation Office at and after sentencing); but see United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004) (remanding for consideration of the details of the government’s proposed computer-monitoring program, to ensure that it is not overly burdensome).
Communications or file transfers. Courts have also imposed Internet access limitations on defendants found guilty of identity theft. Certainly, defendants who have exploited the quick and cheap communications capacity of the Internet to commit investment fraud, especially those who have created phony analyst reports, news sites, or multiple identities to advance their schemes, can reasonably expect to be restricted in their access to the Internet, at least for the duration of their supervised release.

III. NEW TOOLS TO ADDRESS ONLINE INVESTMENT FRAUD

What I have described up until this point tries to capture what is likely to happen in the prosecution of online investment fraud. The fact is, there are few reported cases in this area—and there are good reasons for that. First, since the unfolding of the Enron, WorldCom, and other spectacular financial reporting crimes in 2001 and 2002, many SEC lawyers and financially-sophisticated lawyers at the Department of Justice have been assigned to those high profile cases. Second, prosecuting online investment schemes requires two sets of valuable skills: an understanding of the technology and an understanding of the securities laws. People with both of these skills are valuable outside of government and get recruited away. Third, where the Department of Justice has to prioritize its workload, cybercrimes involving pornography or infrastructure attacks are likely to receive more attention than the ones involving investment schemes.

Still, using the tools at hand, the Department of Justice

---

107 Deborah Solomon, Executives on Trial: Crackdown Puts Corporations, Executives in New Legal Peril, WALL ST. J., June 20, 2005, at A1. Since the formation of the corporate fraud task force in 2002, the Justice Department has charged more than 900 individuals in more than 400 cases. Id.
has generated a significant record in crafting tough sentences for defendants convicted of online investment fraud. 108 In this section of the Article, I want to propose three additional tools that would aid in appropriate sentencing of these defendants. I will also propose an additional device: a public registry designed to deter recidivist offenders.

A. Authorize an Enhancement for Use of a Computer in Perpetrating a Fraud

Let us assume that the use of an interactive website, without more, does not qualify for a "sophisticated means" enhancement. Although I have argued above that it should qualify, there is a plausible argument that it does not. I propose that the Sentencing Guidelines be amended to provide clearly for the availability of a two-level enhancement whenever the Internet is an indispensable element of a federal fraud, securities, or otherwise.

There is already a template for a provision like this. The Sentencing Guidelines already authorize a two-level enhancement if the offense involves a violation of the Computer Fraud and Abuse Act with an "intent to obtain personal information." 109 A similar provision could authorize a two-level enhancement if the offense involves the use of the Internet with an intent to obtain money or other items of value by unlawful means.

To support such a provision, I would offer two possible


arguments: first, use of the Internet to effectuate a fraud is, in effect, a home invasion; second, use of the Internet to effectuate a fraud is similar to using a gun in a crime—it increases exponentially the likelihood that harm will occur.

B. Authorize an Upward Departure for Online Crimes Against the Elderly

Thirteen years ago, Congress recognized the especially pernicious use of telemarketing techniques to prey on elderly, often lonely, victims. The Senior Citizens Against Marketing Scams (or SCAMS) Act provides for a significant upward departure where a telemarketing scheme either victimizes ten or more persons over the age of fifty-five or targets persons over the age of fifty-five.

Today's fraud schemes have taken technology one step further. Rather than relying on costly telemarketing campaigns, promoters now often rely on the use of interactive websites, aided by e-mail communication. Telephone follow-up may or may not be involved in these schemes. Still, the Internet approach operates very much like telemarketing. It permits the promoter to enter the victim's home, slowly build a sense of trust and confidentiality, and then time communications to maximize the likelihood of the victim making an investment decision. It would certainly make sense, at a minimum, to amend the SCAMS Act to incorporate spam e-mail campaigns.

C. Authorize an Enhancement for Investments Made With Funds from a Retirement Account

Oftentimes victims move money from safe into unsafe investments because of the lure of a fraud scheme. It

---

111 Id. § 2326(2)(B).
should matter for purposes of sentencing where the victim’s money came from. The State of Utah recognized this when it distinguished, as a matter of substantive law, between investment schemes generally, and those that involve the receipt of money from any of the following sources: equity in a person’s home, a withdrawal from any individual retirement account, or a withdrawal from any qualified retirement plan.113 The Sentencing Guidelines should be amended to provide for a two-level sentence enhancement where victims’ losses are traceable to a decision to cash in equity in their home, make a withdrawal from an IRA, or make a withdrawal from any qualified retirement plan.

D. Register Securities Law Violators

A final recommendation derives from what we already do with respect to sexual predators and physicians with a history of malpractice or disciplinary complaints: compile a registry and put the public on notice of their history and conduct. Currently, there is no one place for prospective investors to go to check on the bona fides of a person in whose business they are contemplating an investment. A Google search may develop some information about previous stock frauds or other misconduct, but there is no central repository for this information, either at the state or federal level.

One might argue that it is easy for defendants to change their names, or the names of their companies, and that any registry would be imperfect, perhaps misleading. Certainly, name changes and multiple websites are not uncommon. Still, the cost of creating a registry is small, and the existence of a registry, like the existence of “watch out” websites that warn potential investors of the risks of online investments, can

---

113 Utah Code Ann. § 61-1-21 (2005). Thanks to Richard Hamp, Assistant Attorney General in Utah, for directing me to this provision.

114 See Lynn Cowan, Investor Education 101: How to Avoid Scams, Wall St. J., May 9, 2006, at D3 (noting the SEC’s creation of cautionary websites that pose as “can’t fail” investment schemes: when the surfer clicks through to the
only serve as an additional deterrent, both to perpetrators of fraud and to their eager victims.

IV. CONCLUSION

Not long ago, a critic of the Securities and Exchange Commission advocated ratcheting up the criminal enforcement of the securities laws, especially violations involving "boiler rooms, pump and dump schemes, and [the sale of] outright fraudulent securities." Others have suggested that securities law violators—especially recidivist securities law violators—simply are not deterred by the imposition of civil sanctions.

One need not abandon civil sanctions before seeking an optimum strategy for criminal enforcement. In this Article, I have set out a number of the tools that are available to prosecutors of online investment fraud. I have also set out four additional tools that would give criminal enforcement of the securities laws even sharper teeth.