An analysis of fraud on the Internet

C. Richard Baker

The author

C. Richard Baker University of Massachusetts-Dartmouth, North Dartmouth, USA.

Keywords

Internet, Fraud, WWW

Abstract

This paper examines the issue of fraud on the Internet and discusses three areas with significant potential for misleading and fraudulent practices, namely: securities sales and trading; electronic commerce; and the rapid growth of Internet companies. The first section of the paper discusses securities fraud on the Internet. Activities that violate US securities laws are being conducted through the Internet, and the US Securities and Exchange Commission has been taking steps to suppress these activities. The second section of the paper discusses fraud in electronic commerce. The rapid growth of electronic commerce, and the corresponding desire on the part of consumers to feel secure when engaging in electronic commerce, has prompted various organizations to develop mechanisms to reduce concerns about fraudulent misuse of information. It is questionable, however, whether these mechanisms can actually reduce fraud in electronic commerce. The third section of the paper discusses the potential for fraud arising from the rapid growth of Internet companies, often with little economic substance and lacking traditional management and internal controls. The paper examines the three areas of potential Internet fraud mentioned above and suggest ways in which these abuses may be combated.

Electronic access

The current issue and full text archive of this journal is available at

http://www.emerald-library.com

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · pp. 348–359
 · ISSN 1066-2243

Introduction

The growth of the Internet has been accompanied by an increasing number of misleading and fraudulent practices. This paper examines three areas with potential for Internet fraud, including: securities sales and trading; electronic commerce; and the rapid growth of Internet companies. With regard to securities sales and trading, the US Securities and Exchange Commission (SEC) has cited a number of companies and individuals for committing securities violations using the Internet (SEC, 1998). Activities that are prohibited under US securities laws are now being conducted through the Internet, and the SEC is trying to suppress these activities. The first section of the paper discusses a variety of fraudulent schemes that have been observed in the area of securities sales and trading.

Misleading and fraudulent practices in electronic commerce have also been growing in frequency (National Consumers League, 1999; BBC, 1999). Responding to the concerns of participants in electronic commerce, various organizations, including the American Institute of Certified Public Accountants (AICPA), have developed products and services, such as WebTrust, which seek to provide assurance against misuse of information. WebTrust and other similar services are becoming increasingly common in electronic commerce, but there is still the potential for fraudulent misuse of information because such services often do not address the issue of fraud. The second section of the paper discusses the use of assurance services as a means to reduce fraudulent misuse of information in electronic commerce.

The rapid growth of Internet companies also presents an opportunity for misleading and fraudulent practices. Few Internet companies are currently profitable, and while most of these companies are legitimate business enterprises, some have little economic substance. The history of other industries where there has been rapid growth and little economic substance indicates that there is significant potential for fraudulent practices to develop. The third section of the paper addresses the potential for fraud in the rapid growth of Internet companies.

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · 348–359

Fraud in securities sales and trading

While the Internet can be a useful tool for gathering investment information, it can also be the arena for illegal activities. In October 1998, the SEC issued a press release citing 44 companies and individuals for committing securities violations using the Internet (SEC, 1998). According to the SEC press release, the companies and individuals were cited for, among other things, failing to tell investors that they were paid for recommending stocks on the Internet, misrepresenting their independence, issuing false or misleading information about the companies they recommended, and taking advantage of price increases to sell their shares at a profit.

Because the Internet allows information to be communicated easily and inexpensively to a wide audience, it is relatively easy for persons intent on committing fraud to send credible looking messages to many potential investors. Investors are often unable to tell the difference between legitimate and false claims. Some of the ways that securities frauds have been committed using the Internet include: online investment newsletters, bulletin boards, and e-mail spam. Many of the frauds cited by the SEC are classic investment frauds, such as: "The pump and dump"; "The pyramid"; "The risk-free fraud"; and "Off-shore frauds" (SEC, 1998).

Online investment newsletters

Many investment newsletters have appeared in recent years on the Internet. Online newsletters can help investors to gather investment information, but in some situations companies pay newsletters to recommend their stocks. This practice is not illegal, but the US securities laws require the newsletters to disclose who paid them, the amount, and the type of payment. If the newsletter does not disclose its relationship with the company being recommended, the newsletter has violated the law. Some online newsletters commit securities fraud by claiming to perform research on the stocks they recommend when in fact they do not. Other newsletters spread false information or promote worthless stocks. The goal is to drive up the price of the stock in order to sell at a higher price (SEC, 1998).

Bulletin boards

Online bulletin boards exist in several different formats including newsgroups, usenet, and Web-based. Bulletin boards have become a popular way for investors to share information, including messages concerning investment opportunities. While many messages are true, some are misleading or fraudulent. Persons may pretend to reveal inside information about upcoming announcements, new products, or lucrative contracts. It may be difficult to ascertain the reliability of such information because bulletin boards allow users to hide their identity behind aliases. People claiming to be unbiased observers may actually be company insiders, large shareholders, or paid promoters. A single person can create the illusion of widespread interest in a small, thinly-traded stock by posting a series of messages under aliases (SEC, 1998).

E-mail spam

E-mail spam is similar to junk mail. Because e-mail spam is inexpensive and easy to create, persons intent on committing securities fraud use it to locate potential investors for investment schemes or to spread false information about a company. E-mail spam allows perpetrators of fraud to target more potential investors than cold calling or mass mailing. Through the use of bulk e-mail programs, personalized messages can be sent to thousands of Internet users simultaneously (SEC, 1998).

Classic investment frauds using the Internet

Investment schemes using the Internet are often similar to those previously seen using the telephone or the mails. Investment schemes generally fall into one of the following categories:

- *The pump and dump* – this type of violation involves online messages that urge investors to buy a stock quickly or recommend selling before the price goes down. The sender of the message usually claims to have inside information about a company or the ability to pick stocks that will increase in price. The perpetrators of the fraud may be insiders or paid promoters who stand to gain by selling their shares after the stock price is pumped up. Once the perpetrators

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · 348–359

sell their shares and stop hyping the stock, the price usually falls and investors lose their money. This scheme is usually employed with small, thinly-traded companies because it is easier to manipulate a stock when there is relatively little information available about the company.

- *The pyramid* – this type of scheme involves a message such as: "How to make big money from your home computer!!" An example might be when the message claims that investors could turn $5 into $60,000 in just three to six weeks. This is an electronic version of the classic pyramid scheme where participants make money only by recruiting new participants into the program. Eventually the pyramid collapses and the investors lose their money.
- *The risk-free plan* – This type of scheme involves a message like: "Exciting, low-risk investment opportunities" inviting participation in: wireless cable projects, prime bank securities, or eel farms. The investment products typically do not exist.
- *Off-shore frauds* – off-shore schemes often target investors in another country to avoid the jurisdiction of securities laws. Because the Internet has removed barriers imposed by different time zones, different currencies, and the high costs of international telephone calls and mailings, when an investment opportunity originates in another country, it is difficult for law enforcement agencies to investigate and prosecute the frauds.

Examples of securities fraud using the Internet

(1) The SEC cited Francis Tribble and Sloane Fitzgerald, Inc. for sending more than six million unsolicited e-mails, building false Web sites, and distributing an online newsletter to promote the stock of two small, thinly traded companies. Because Tribble and Sloane failed to tell investors that the companies agreed to pay them in cash and securities, the SEC sued and imposed a $15,000 penalty on Tribble. The massive amount of spam distributed by Tribble and Sloane resulted in hundreds of complaints being received by the SEC's online Enforcement Complaint Center (*SEC* v. *Tribble*, 1998).

(2) The SEC also cited an online newsletter called *The Future Superstock* (FSS), written by Jeffrey Bruss of West Chicago, Illinois, who recommended the purchase of micro-cap (i.e. small capitalization) stocks predicted to double or triple in the months following the recommendations. In making these recommendations, FSS:
   - failed to disclose more than $1.6 million of compensation, in cash and stock, from the issuers;
   - failed to disclose that it had sold stock in many of the issuers shortly after the recommendations caused the prices of those stocks to rise;
   - had not performed independent research and analysis in evaluating the issuers profiled by the newsletter; and
   - lied about the success of certain prior stock picks (*SEC* v. *The Future Superstock et al.,* 1998).

(3) In a third citation, the SEC said that John Wesley Savage and Princeton Research, Inc. touted the stocks of seven different companies while receiving 276,500 shares and 75,000 options from those companies. Savage and Princeton also lied about the financial condition of two of the issuers. Savage and Princeton consented to a permanent injunction and payment of a civil penalty of $40,000 (*SEC* v. *John Wesley Savage et al.,* 1998).

(4) The SEC also cited Charles Huttoe and 12 other defendants for secretly distributing to friends and family nearly 42 million shares of Systems of Excellence Inc., known by its ticker symbol SEXI. In a pump and dump scheme, Huttoe drove up the price of SEXI shares through false press releases claiming multi-million dollar sales which did not exist, an acquisition that had not occurred, and revenue projections that had no basis in reality. He also bribed co-defendant, SGA Goldstar, to tout SEXI to subscribers to SGA Goldstar's online newsletter called Whisper Stocks. The SEC fined Huttoe $12.5 million. Huttoe and Theodore Melcher, the author of the online newsletter, were sentenced to federal prison. In

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · 348–359

addition, four of Huttoe's colleagues pled guilty to criminal charges (SEC, 1998).

(5) Matthew Bowin recruited investors for his company, Interactive Products and Services, in a direct public offering done entirely over the Internet. Bowin raised $190,000 from 150 investors. Instead of using the money to build the company, Bowin pocketed the proceeds. The SEC sued Bowin in a civil case, and the Santa Cruz, California, District Attorney's Office prosecuted him criminally. He was convicted of 54 felony counts and sentenced to jail (SEC, 1998).

(6) IVT Systems solicited investments to finance the construction of an ethanol plant in the Dominican Republic. The Internet solicitations promised a return of 50 per cent or more with no reasonable basis for the prediction. The solicitations included false information about contracts with well-known companies and omitted other important information about the company (SEC, 1998).

(7) Gene Block and Renate Haag were cited by the SEC for offering prime bank securities through the Internet, a type of security that does not exist. Block and Haag collected over $3.5 million by promising to double investors' money in four months. The SEC froze their assets and prevented them from continuing their fraud (SEC, 1998).

(8) Daniel Odulo was found to be soliciting investors for a proposed eel farm. Odulo promised investors a 20 per cent return, claiming that the investment was low risk. He consented to a court order stopping him from breaking the securities laws (SEC, 1998).

Addressing securities fraud on the Internet

Securities schemes using the Internet are usually similar to ones previously seen using other media. The perpetrators of such schemes often engage professional advisors for counsel concerning accounting, tax, legal, information systems and other matters. It is important that professional advisors be aware of the full range of activities of their clients. If the client's activities include securities violations using the Internet, the advisor should counsel their clients to avoid such activities. If the client does not respond appropriately, the advisor should cease further contact with the client. Obviously, if the advisor is facilitating such activities they will be subject to legal enforcement actions or even criminal prosecution.

Professional advisors may also provide advice and counsel to their clients about investments. Avoiding fraudulent schemes is an area where advisors can be of great assistance to their clients. In order to invest wisely, it is important to obtain accurate and reliable information. Investments should not be made based solely on information appearing in an online newsletter or bulletin board, especially if the investment involves a small, thinly-traded company that is not well known. Investing in small companies that do not file regular public reports should be avoided, unless you are willing to investigate the company and thoroughly check the truth of every statement about the company. Examples of steps that should be taken are to:

- obtain financial statements directly from the company and analyze them thoroughly;
- verify the claims about new product developments or lucrative contracts;
- call suppliers and customers of the company and ask if they really do business with the company; and
- check out the people running the company and find out their track record.

The US federal securities laws require most public companies to register with the SEC and file annual and quarterly reports containing audited financial statements. All US companies with more than 500 investors and $10 million in net assets and all companies that list their securities on the Nasdaq Stock Market or a major national stock exchange such as the New York Stock Exchange must file reports with the SEC. Anyone can access and download these reports from the SEC's EDGAR database through the Internet. It is important to check whether the company is registered with the SEC and read the reports that are filed with SEC.

Electronic commerce and Internet fraud

The Internet has become an increasingly powerful way to conduct business (Tedeschi, 1999). Forrester Research, Inc. indicates that participants in electronic commerce exchanged

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · 348–359

$8 billion over the Internet in 1997 and will exchange well over $100 billion by the year 2000 (Forrester Research, 1999). The US Department of Commerce predicts that business-to-business electronic commerce will reach $300 billion by 2002 (Department of Commerce, 1998). Most transactions involving electronic commerce are consummated with credit cards or bank charges. The use of credit cards in electronic commerce provides a certain amount of assurance to consumers because there are legal limits on liability for unauthorized use of credit card information. Nevertheless, perpetrators of fraudulent and misleading practices often look for opportunities to obtain credit card information as well as other private information such as e-mail addresses, personal addresses, phone numbers, birth dates, social security numbers, and so forth, which can be sold to e-mail spam lists. Consequently, this is an area which is ripe for fraud.

Many participants in electronic commerce are concerned about the potential for fraudulent practices. The US National Consumers League indicates that one of the primary concerns of consumers is in regard to online auctions and the potential for lack of receipt of products or services paid for or receipt of products or services of lesser quality than bargained for (National Consumers League, 1999). Gray and Debreceny (1998) also indicate some of the concerns that participants in electronic commerce have, including:

- Is this a real company?
- Is this a trustworthy company?
- If I send credit card or bank information, is it safe?
- If I provide information to a company on its Web site, where will the information end up?
- If I place an order, will I receive what I asked for?
- Will I receive delivery when promised?
- Will any problems I have be resolved quickly?
- Is a money-back guarantee honored?
- How soon will I get credit for returned items?
- How quickly will the company perform service on warranty items?
- Will the company be able to send me necessary replacement parts quickly?

The concerns expressed above can exist with any transaction, whether conducted face-to-face, over the telephone, through the mail, or over the Internet. Unscrupulous people will be unscrupulous regardless of the medium through which the transaction is conducted.

Several mechanisms have been created in recent years to reduce the concerns of participants in electronic commerce, including electronic logos, encryption techniques and firewalls. The idea behind an electronic logo is that if an Internet seller meets certain specified criteria, the seller is allowed to place a logo on its Web site. The logo is provided by an assurance provider, such as a public accounting firm, or another entity organized for this purpose. The logo provides a certain level of assurance that the seller has complied with standards established by the assurance provider. Usually, the logo is linked to the assurance provider's Web site. The Internet user can link to the assurance provider's Web site to read about the degree of assurance provided by the logo (Gray and Debreceny, 1998).

Logo assurance services are becoming quite common. For example, MasterCard and Visa created secure electronic transactions (SET). Companies selling products or services through the Internet that meet SET standards for sending credit card information can display the SET logo (see www.visa.com). The assurance provided by the SET logo relates primarily to the idea that the credit card information cannot be easily intercepted during the process of transmission from buyer to seller. In a similar manner, the VeriSign logo (www.verisign.com) provides assurance to consumers that a Web site is capable of transmitting and receiving secure information and that the site and company are real. The SET and VeriSign logos focus on the security of the transaction and the validity of the Web site and the vendor.

WebTrust is another logo assurance service that was developed jointly between the American Institute of CPAs (AICPA) and the Canadian Institute of Chartered Accountants (CICA). Accounting associations in the UK, Australia and New Zealand are also planning to participate in the WebTrust logo assurance program. WebTrust operates under the assumption that consumers seek assurance in the following areas:

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · 348–359

- They are dealing with a real company, rather than a fraudulent company seeking to obtain and sell credit card numbers, addresses, and other private information.
- They will receive the goods and services ordered, when promised, at the agreed-on price.
- They have the option to request that the Internet seller not give or sell any private information provided in an online transaction.
- Private information cannot be intercepted while being transmitted (Primoff, 1998).

To obtain a WebTrust logo, an Internet seller must meet criteria in three areas:
(1) business practices disclosure;
(2) transaction integrity; and
(3) privacy and information protection.

Business practices disclosure
The purpose of the disclosures in this area is to provide assurance to consumers that they are dealing with a real business that abides by its promises. The disclosures relate to several business practices, such as delivery times, product return policies, and warranty information. Unfortunately, the seller is not required to follow any specific practices. However, before issuing a WebTrust logo the assurance provider must verify that disclosed practices are being followed by the seller. One item of disclosure that is required is that the Web site must include the seller's postal address and telephone number.

Transaction integrity
In this area, assurance is provided that internal controls are in place so that customer orders are recorded and billed properly. The assurance provider is primarily concerned with customer oriented controls rather than those related to financial statements.

Privacy and information protection
In this area, assurance is provided that private customer information is not misused by company insiders and that controls are in place to keep information secure from unauthorized parties during and after transmission. WebTrust also requires that sellers be re-certified every 90 days (Gray and Debreceny, 1998; Primoff, 1998).

Although the WebTrust program has the potential to combat fraud on the Internet, the start up of the WebTrust logo has been slow. As of May 1998, only 1,500 CPAs had been trained by the AICPA, and 65 firms were licensed to issue the WebTrust logo (Cahners Publishing Company, 1998). It is unclear whether this slow start is due to a reluctance on the part of accounting firms to offer the service or whether there is a lack of demand for the WebTrust product. Gray and Debreceny (1998) suggest that the primary market for WebTrust services will be new, Internet based sellers without well established reputations. Consumers are reluctant to enter into Internet transactions with sellers with whom they are not familiar. Consequently, an assurance logo located on the Web site of the Internet seller can be a marketing tool. At the same time, accounting firms may not be comfortable selling WebTrust services to the marketing departments of their clients.

An example of a WebTrust application

In October 1998, the AICPA issued a press release indicating that Bennett Gold, a Canadian Chartered Accounting firm, had provided a WebTrust logo to Competitor Communications, Inc., an Internet service provider for the RocketRoger.com Web site (AICPA Press Release 1998). RocketRoger.com (www.RocketRoger.com) is a Web site established for fans of Roger Clemens, a well-known baseball player. In addition to information about the career of Roger Clemens, the Web site offers visitors the opportunity to purchase Roger Clemens memorabilia using credit cards. The RocketRoger.com Web site was the first Canadian Web site to receive the WebTrust logo (AICPA Press Release, 1998). Bennett Gold, which is based in Toronto, Canada, issued the logo for the RocketRoger.com Web site after performing a WebTrust audit. In a WebTrust audit, an accounting firm examines an Internet company to determine if the business is legitimate, its transactions are secure, the information it collects from consumers is kept private, and its business practices are fully disclosed (AICPA Press Release, 1998). Table I contains a copy of the audit report issued by

Table I WebTrust auditors report

To: The Management of Competitor Communications Incorporated

We have audited Competitor Communications Incorporated's disclosure of its electronic commerce business practices on its Web site and the effectiveness of its controls over transaction integrity and information protection for electronic commerce (at www.competitor.net) during the period of May 1, 1998 through April 15, 1999. These electronic commerce disclosures and controls are the responsibility of Competitor Communications Incorporated's management. Our responsibility is to express an opinion on the conformity of those disclosures and controls with the AICPA/CICA WebTrust criteria based on our audit.

We conducted our audit in accordance with standards for assurance engagements established by the Canadian Institute of Chartered Accountants. Those standards require that we plan to perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of Competitor Communications Incorporated's electronic commerce business practices and its controls over the processing of electronic commerce transactions and the protection of related private customer information, (2) selectively testing transactions executed in accordance with the disclosed business practices, (3) testing and evaluating the operating effectiveness of the controls, and (4) performing such other procedures as we considered necessary in the circumstances.

In our opinion, during the period May 1, 1998 through April 15, 1999, Competitor Communications Incorporated in all material respects:

- disclosed its business practices for electronic commerce transactions and executed transactions in accordance with its disclosed business practices,
- maintained effective controls to provide reasonable assurance that customers' orders placed using electronic commerce were completed and billed as agreed, and
- maintained effective controls to provide reasonable assurance that private customer information obtained as a result of electronic commerce was protected from uses not related to Competitor Communications Incorporated's business in accordance with the AICPA/CICA WebTrust criteria.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods are subject to the risks that (1) changes made to the system or controls, (2) changes in the processing requirements, or (3) changes required because of the passage of time, such as to accommodate dates in the year 2000, may alter the validity of such conclusions.

The CA WebTrust seal of assurance on Competitor Communications Incorporated's competitor.net Web site for electronic commerce constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of Competitor Communications Incorporated's goods or services at the www.competitor.net Web site nor their suitability for any customer's intended purpose.

BENNETT GOLD
Chartered Accountants
April 16, 1999
Toronto, Ontario, Canada
www.BennettGold.ca

Bennett Gold regarding the RocketRoger.com Web site.

The audit report issued by Bennett Gold is similar to a standard audit report issued for an audit of financial statements; however, it is important to note that there is an explicit disclaimer of responsibility for fraud. Consequently, even though the WebTrust logo assurance program may help to reduce consumers' fears about fraud, there is a low level of assurance being provided about the possibility of fraud.

Combating fraud in electronic commerce

The use of logo assurance services and other forms of encryption techniques may help to reduce the level of misleading and fraudulent practices in electronic commerce. Professional

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · 348–359

advisors should urge their clients who are buyers of products or services through the Internet to be aware of the presence or absence of logos on the Web sites of the companies with whom they deal, and they should encourage their clients to deal with sellers who have logos from reputable assurance providers. In addition, both professional advisors and their clients should be familiar with the limits on the level of assurance provided by these logos. It is also important to realize that providers of the WebTrust logos generally disclaim responsibility if the Internet company violates the criteria of the WebTrust logo or if fraud is being perpetrated. Consequently, the logo assurance program should be used cautiously in conjunction with other forms of protection against misleading and fraudulent practices. Furthermore, in the case of online auctions, there is little protection against misleading or fraudulent practices, especially if the products or services are not as advertised or never delivered. Consequently, it is important to exercise caution when dealing in electronic commerce.

Potential fraud in the growth of Internet companies

A third potential area for fraudulent and misleading practices on the Internet lies in the rapid growth of companies, particularly those whose existence depends entirely on the World Wide Web. Even though growing very rapidly, electronic commerce is still developing. There are many entrepreneurs striving to become established on the Internet. Ultimately many of these companies will fail. During a period of rapid growth and subsequent contraction in an industry, there are likely to be fraudulent practices emerging. Even if most Internet companies are legitimate, some have no economic basis. The business practices of some Internet companies border on fraud. In addition, as with other rapidly growing industries, there is often a lack of control over systems and data, particularly when a significant portion of a company's transactions are conducted through the Internet. Internet companies often use Internet Service Providers (ISPs) to maintain Web sites, process transactions, and maintain catalogs of merchandise (Primoff, 1998). In this environment, Internet companies may not have control over systems and data that are essential to their business. This is an environment ripe for fraud.

The Internet is often viewed as a rainbow with a pot of gold at the end. However, there is a grim reality to this picture. Most Internet companies do not make money (Hansell, 1998; Kedrosky, 1998). Even Amazon.com, one of the best known Internet companies, has not made a profit since its inception (see Table II). Currently, the economic basis of many Internet companies is not in the sale of products or services but in the sale of advertising. Many Internet companies are created on the basis of projections about advertising revenue drawn from market research done by consulting firms. These projections may be suspect for several reasons. As with other forms of advertising, Internet advertising revenue is based on the number of persons who view the advertisement. However, it is estimated that the top ten Internet sites receive 50 per cent of the advertising revenue, and the top 100 sites receive almost 95 per cent of the revenue (Kedrosky, 1998).

A second area in which projections concerning Internet advertising revenue may be suspect lies in the area of banner exchanges. Internet companies earn advertising credits by running advertisements for other Internet companies. In other words, one Internet company provides advertising for another Internet company and vice versa. The payments are in the form of credits for advertising on the other company's Web site. Revenues are produced, but there is no cash flow (Kedrosky, 1998).

A third area in which Internet advertising revenues may be suspect lies in the measurement of the number of visitors to a Web site. A Web site may report that it receives one million hits (i.e. visitors). However, the number of actual visitors may be as low as one percent of that number (i.e. 10,000). This is because the measurement of hits is based on factors such as the number of links and graphic images on the site. Consequently, the number of actual visitors is difficult to measure with any degree of accuracy (Kedrosky, 1998).

Beyond the issue of questionable projections concerning Internet advertising revenues, there is the issue of new technologies such as autonomous agents which may reduce the

Table II Amzazon.com, Inc. Consolidated statements of operations (in thousands, except per share data)

	Years ended 31 December		
	1998	**1997**	**1996**
Net sales ($)	609,996	147,787	15,746
Cost of sales	476,155	118,969	12,287
Gross profit	133,841	28,818	3,459
Operating expenses:			
Marketing and sales	133,023	40,486	6,090
Product development	46,807	13,916	2,401
General and administrative	15,799	7,011	1,411
Merger and acquisition related costs, including amortization of goodwill and other purchased intangibles	50,172	–	–
Total operating expenses	245,801	61,413	9,902
Loss from operations	(111,960)	(32,595)	(6,443)
Interest income	14,053	1,901	202
Interest expense	(26,639)	(326)	(5)
Net interest income (expense)	(12,586)	1,575	197
Net loss ($)	(124,546)	(31,020)	(6,246)
Basic and diluted loss per share ($)	(0.84)	(0.24)	(0.06)

Source: (edgar.sec.gov/Archives/edgar/data/1018724/0000891020-98-000448.txt)

chances of earning a profit from Internet sales. The purpose of an autonomous agent is to locate every seller on the Internet that sells a particular item and then to sort them by price. Consequently, whatever an Internet company tries to do to create brand identity, or provide service, autonomous agents will drive towards the lowest price (Kedrosky, 1998). In addition, it is questionable whether Internet companies are making money even in the current robust environment of rapidly growing Internet commerce. It is estimated that despite large increases in Internet commerce during 1998, less than 5 per cent of online retailers earned a profit (High, 1999).

Another area with potential for fraud on the Internet lies in the initial public offering of Internet company shares. During 1998 and 1999, there was a stock market fascination with Internet companies which resembled a speculative bubble. Internet companies with no earnings, and in some cases no sales and even negative net worth, completed IPOs at highly inflated prices. Table III contains some examples of Internet IPOs. One example of an Internet IPO was Ebay, which closed on December 28, 1998 nearly 1,500 per cent higher than its initial public offering price on September 24, 1998. The price earnings ratio of Ebay has exceeded 6,500, and its price to book ratio has exceeded 120. Because of the lack of earnings of most Internet company IPOs, analysts are using price to sales ratios as a comparative indicator. It seems probable that the lack of economic substance underlying many Internet IPOs will result ultimately in a decline in the price of Internet company shares.

A final area of potential fraud arising from the rapid growth of Internet companies lies in the lack of managerial and internal controls in these companies. Until recently, the cost of the hardware, software, and professional expertise necessary for electronic commerce served as a barrier to entry. The costs are now much lower. Internet service providers (ISPs) offer turnkey solutions that combine hardware, software, payment processing, and communications in one package. Since the ISP packages are outsourced, they operate solely on the ISP's computers (Primoff, 1998). In a turnkey ISP approach, all of the information is located with the ISP, but the Internet company needs access to the information, and the ability to exclude unauthorized persons from obtaining access. It is important for companies to understand how the information is controlled and by whom. It is

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · 348–359

Table III Selected Internet IPOs

Company	Offer date	Percentage price change to 12/28/1998 (%)	PE ratio	Price sales ratio	Price book ratio
Ebay	9/24/98	+1,488.9	6486.49	236.69	117.89
Ubid	12/03/98	+710.9	neg.	neg.	neg.
Broadcast.com	7/16/98	+424.3	neg.	85.38	22.04
TicketmasterOnline-CitySearch	12/02/98	+367.9	neg.	neg.	12.55
Theglobe.com	11/12/98	+322.2	neg.	12.16	5.31
Tricom	5/04/98	–50.5	11.67	7.84	4.13
Genesis Direct	5/07/98	–59.2	neg.	0.82	1.73
Asymetrix Learning Systems	6/12/98	–65.9	neg.	1.47	2.01
Ursus Telecom	5/13/98	–67.1	neg.	neg.	1.31
USN Communications	2/03/98	–99.0	neg.	0.03	neg.

Source: Hansell (1998); Yahoo! (biz.yahoo.com/i/)

also important to ascertain whether the Internet company and the ISP personnel have the skills necessary to deal with issues of security and internal control and what security techniques are employed (Primoff, 1998).

Discussion

Within a relatively short period of time the Internet has developed into a powerful medium of communication and human interaction. Unfortunately, the growth of the Internet has been accompanied by an increasing incidence of fraudulent and misleading practices. This paper has discussed three areas with potential for fraud on the Internet. It is likely that others will develop. The purpose of this section is to suggests some commonalities among the previous discussion of three potential areas for fraud.

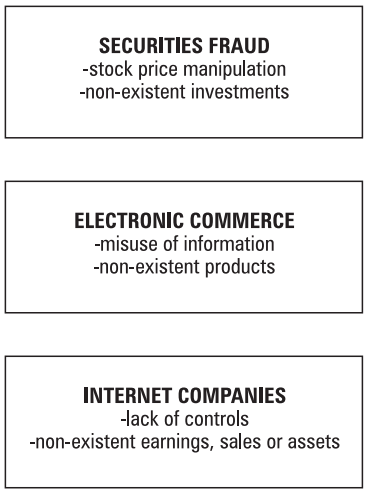
In the first area of commonality, it appears that the low cost, the high speed, and the anonymity of the Internet may have allowed a new type of fraud to develop, one in which barriers to engaging in misleading practices are low and insignificant. Prior to the Internet, the cost of sending misleading information through the mails or by making telephone solicitations, may have acted as an impediment to such schemes. In the USA and other countries, there have been specific laws against mail fraud for many years, but the laws against Internet fraud are still developing. The SEC can only pursue securities violations that occur in the USA. The Internet is a global information system, and there is no global securities regulator. Hence, fraudulent and misleading securities schemes can operate relatively unchecked in cyberspace. The same holds true for electronic commerce. There is no global regulation of online commerce, and Internet companies are global operators. Fraudulent and misleading practices tend to develop in situations without controls. In an unregulated medium the potential for fraud is great. Does this mean that the Internet should be regulated? Perhaps not. But, fraudulent and misleading practices should be regulated. This means that law enforcement agencies must have the ability to investigate and pursue violations of law wherever they may occur.

Second, in each of the areas discussed, there is an element of credulity. In another words, the misleading practices could not take place without the willing suspension of disbelief on the part of securities investors, electronic consumers, and purchasers of Internet company IPOs. If something looks too good to be true, it usually is. If someone suggests in an Internet chat group that they have inside information about a company, they probably do not. If they offer something in an on-line auction at a price below value, either the value or the item are probably not there. If someone buys an Internet IPO and expects to become an instant millionaire, they probably won't.

Table IV presents a summary of the findings of this paper. In this table it becomes reasonably apparent the that the primary reason for the

Internet Research: Electronic Networking Applications and Policy
Volume 9 · Number 5 · 1999 · 348–359

Table IV Potential areas for fraud on the Internet



advent of fraud on the Internet is a lack of controls combined with a high degree of credulity on the part of participants in the securities markets and electronic commerce. While it is difficult to recommend that controls should be imposed on the Internet, if fraudulent and misleading practices are perceived to be an important issue, then some form of controls ought to be implemented. At the same time, it is important to recognize that the lack of prudence on the part of many investors and participants in electronic commerce has presented unscrupulous operators with an unprecedented opportunity to commit fraud.

Conclusion

This paper has examined the question of fraud on the Internet and has examined three areas with significant potential for fraud. These include:

(1) securities fraud;
(2) fraud in electronic commerce; and
(3) fraud arising from the rapid growth of Internet companies.

The SEC has cited a number of companies and individuals for committing securities violations on the Internet. Activities prohibited under US law are being conducted through the Internet, and the SEC is taking action to suppress these activities. A second potential area for fraud on the Internet discussed in this paper lies in electronic commerce. The growth of electronic commerce in recent years, and the corresponding desire by consumers to feel secure when engaging in electronic transactions, has prompted the AICPA to create WebTrust, which may help to reduce concerns about fraudulent use of information. A third area for potential fraud on the Internet discussed in this paper involves the rapid growth of Internet companies, often based on little economic substance and without traditional management or internal controls. The expansion of Internet commerce is a development that is perceived to be beneficial for society; consequently it is important that fraud on the Internet be combated.

References

AICPA News Release (1998), "Rocketroger.com and Roger Clemens hit grand slam with CA WebTrust seal of assurance", press release issued by the American Institute of CPAs, New York, NY, 30 September.

BBC (1999), "Internet scam file", BBC On-line Network, 7 April, news.bbc.co.uk/hi/english/business/your_money/newsid_313000/313051.stm.

Cahners Publishing Company (1998), "Auditing the Web-site", *Electronic News*, Vol. 44 No. 2219, p. 48.

Department of Commerce (1998), *The Emerging Digital Economy*, US Department of Commerce, Washington, DC.

Forrester Research (1999), www.forrester.com.

Gray, G.L. and Debreceny, R.S. (1998), "The electronic frontier", *Journal of Accountancy*, Vol. 185, May, pp. 32-7.

Hansell, S. (1998), "A quiet year in the Internet industry", *The New York Times*, 28 December, p. C1.

High, K. (1999), "What the holiday Web boom hid", *Fortune & Your Company*, 4 January, cgi.pathfinder.com/yourco/briefs/0,2246,142,00.html.

Kedrosky, P. (1998), "There's little but fool's gold in the Internet boomtown", *The Wall Street Journal*, 23 November, p. A22.

National Consumers League (1999), *Internet Fraud Watch*, www.nclnet.org/Internetscamfactsheet.html.

Primoff, W.M. (1998), "Electronic commerce and Webtrust", *The CPA Journal*, Vol. 68 November, pp. 14-23.

SEC (1998), *Internet Fraud: How to Avoid Internet Investment Scams*, US Securities and Exchange Commission, Washington, DC, October, www.sec.gov/consumer/cyberfr.htm.

SEC v. *John Wesley Savage et al.* (1998), www.sec.gov/enforce/litigrel/lr15954.txt.

SEC v. *The Future Superstock et al.* (1998), www.sec.gov/enforce/litigrel/lr15958.txt.

SEC v. *Tribble* (1998), www.sec.gov/enforce/litigrel/lr15959.txt.

Tedeschi, B. (1998), "Real force in e-commerce is business-to-business sales", *New York Times Online*, 5 January www.nytimes.com.

Further reading

Garcia, A.M. (1998), "Global e-commerce explodes: will you thrive, survive, or die?", *e-Business Advisor*, October.
Lohr, S. and Markoff, J. (1998), "AOL lays out plan for marriage to Netscape", *New York Times On-line*, 28 November, www.nytimes.com.
Nagel, K.D. and Gray, G.L. (1998), *Guide to Electronic Commerce Assurance Services*, Harcourt Brace Professional Publications, Orlando, FL.
Schmidt, W. (1998), "WebTrust services: AICPA launches WebTrust for assurance", *The CPA Journal*, Vol. 5, p. 70.

(C. Richard Baker is an Associate Professor in the Department of Accounting and Finance. In addition to prior academic positions at Columbia, Fordham, and St John's Universities, Dr Baker has had over 12 years experience in business and corporate finance He has been an audit manager with the National Office of a Big 5 accounting firm, a vice president with several investment banks, and vice president and controller for an energy development company.

Dr Baker has co-authored six books dealing with accounting, finance and taxation. He is also the author of over 40 academic and professional papers. He is an active member of the public accounting profession having served on committees of the American Institute of CPAs, the New York State Society of CPAs and the American Accounting Association. He has been a frequent speaker and presenter of papers at professional meetings. Dr Baker has also served as financial advisor and consultant to development stage companies and has been an expert witness on accounting matters in several legal proceedings. His current research interests are focused on the legal and ethical aspects of the public accounting profession and on specialized financing practices. Dr Baker holds a PhD in Accounting from UCLA. He is also a Certified Public Accountant in New York State.)