An Examination of Internet Fraud Occurrences

Kai S. Koong

The University of Texas - Pan American
Computer Information Systems and Quantitative Methods Department
1201 West University Drive, Edinburg, Texas 78541-2999, USA
Phone: 956-381-3353 Fax: 956-381-3367
E-mail: koongk@utpa.edu

Lai C. Liu

The University of Texas - Pan American
Computer Information Systems and Quantitative Methods Department
1201 West University Drive, Edinburg, Texas 78541-2999, USA
Phone: 956-381-3353 Fax: 956-381-3367
E-mail: liul@utpa.edu

June Wei

University of West Florida
Department of Management and Management Information Systems
Pensacola, Florida 32514, USA
Phone: 850-474-2316
E-mail: jwei@uwf.edu

ABSTRACT

As a result of Internet technology, transactions processing has undergone remarkable changes. On the positive side, e-commerce, m-commerce, and l-commerce have become a reality in the electronic marketplace. However, one of the undesirable outcomes of the Internet is its use for criminal acts. This study examines the proliferation of Internet fraud for the period 1998 through 2002. Specifically, the variables examined included the categories of online fraud, payment methods used for committing those frauds, the affected victims, and trends, if any. The results of this study should be of interest to all types of individuals involved in law enforcement, computer and information systems security designers, and especially consumers of online systems. Computing educators in particular will find the outcomes reported in this study useful because they can be used to develop and design curriculum and course content that can help minimize online fraud. In addition, the exhibited trends on Internet fraud and the major means used by criminals can be used to educate the growing number of students who are using the Internet for their shopping needs as well as other personal activities.

INTRODUCTION

Three major developments around the globe have enabled businesses to better reach prospective consumers. First, computer ownership around the globe has exceeded 625 million. The United States alone has about a third of those computers (Petska, 2001). Second, advances in Internet related technologies have enabled businesses to better communicate services and products to

targeted audiences. Customers can now preview products online in multimedia format. Prior to the new millennium, some 80 percent of all Internet use was already graphic intensive (DeVeaux, 1999). Third, consumers are getting savvy and comfortable buying online. Apart from the demand for information access, the increase in Internet traffic is indeed brought about by the proliferation in the demand for services and products (Theel, Stephens, and Easland, 2001).

While it is true that most online companies are legitimate and honest in their business practices, Internet technology has also attracted the attention of computer technology savvy criminals. Given the many e-mail solicitations received daily and relative ease of setting up and closing up a Website with transaction processing capability, consumers can easily become victims to online fraud. In a nutshell, online fraud is any type of fraud scheme that uses one or more components of the Internet to perpetuate a crime. Such means may include chat rooms, message boards, or Websites. It is broadly defined as online fraud when an Internet component is used (a) to present fraudulent solicitations to prospective victims, (b) to conduct fraudulent transactions, or (c) to transmit the proceeds of fraud to financial institutions or to others connected with the scheme (U. S. Department of Justice, 2003).

Fraud is not a new phenomenon because it has always been around since human history. Its definition and outcomes on victims have not changed. With the use of the Internet for commercial purpose, the method of perpetration of fraudulent activities has evolved to include online capabilities (Lee, 2003). In other words, the Internet has opened up a door for the development of a new criminal sector of fraud. The scary aspect of this type of new fraud is that perpetrators can now use the anonymous advantage of the Internet to cause harm (PBI Media, 2003). Since the Internet works on real time, a prospective victim can be harmed much more easily and quickly. It is even possible for the criminal to harm the same victim again and again because the fraudulent electronic transactions can be repeatedly processed within a short period of time. Therefore, conventional wisdom requires that a consumer be always cautious and knows what to watch out for when buying online (Trebilcock, 1998).

STATEMENT OF THE PROBLEM

While some of the early cases of Internet fraud can be traced to 1996, little details about them were available. It was not until 1997 that documented cases of Internet fraud became available (Internet Fraud Watch, 1997). Since then, both the number of cases and the type of crimes have continued to multiply, and the means for committing those criminal acts have also continued to evolve (Laurent, 1997). In 2002 alone, the Internet Fraud Compliant Center reported that some seventy-five thousand complaints were received (Bennet, 2003). Compared to 2001, Internet fraud was found to have tripled in just one year (Associated Press, 2003). Dollars reported paid in enforcement actions against Internet scams alone totaled $122.3 million (U.S. Federal Trade Commission - Bureau of Consumer Protection, 2003).

Internet fraud is a growing problem. First and foremost, consumers around the world are becoming more and more comfortable with e-commerce practices. Second, online services are becoming more ubiquitous so the volume of m-commerce activity could easily equal those of e-business soon. However, there is no governing or professional authority that has the ability or

capability to certify and monitor Web content. Drawing from the dramatic increases in fraud reports in the recent few years, Internet fraud is definitely expected to rise as the amount of commerce increases on the Net (Manuel, 1999).

STATEMENT OF OBJECTIVE

While it is true that cyber criminals can use Internet technologies to target all prospective online users and business activities, its effectiveness can be rather diverse. Certain demographic user categories may be more vulnerable than others. Some business applications may also be more prone to fraud. This study examines the proliferation of Internet fraud for the period 1998 through 2002. Specifically, the variables examined included the categories of online fraud, payment methods used for committing those frauds, the affected victims, and trends, if any.

Knowledge pertaining to the type of techniques, applications, and people group harmed can help governmental agencies to be more effective in their enforcement efforts and to provide the proper advice the public may need. The results of this study should also be of interest to all users of online systems and individuals involved in computer and information systems security design and development. Computing educators in particular, can use the outcomes reported in this study for the development and design of new curriculum and course content that can help to minimize computer crimes. In addition, the exhibited trends on Internet fraud and the major means used by criminals can also be used to educate students about the risks associated with online activities.

METHODOLOGY

Data for this study was obtained from The Internet Fraud Watch (IFW) project's annual reports. The IFW is a project that operates in tandem with the National Consumers League's National Fraud Information Center (NFIC) located in Washington, District of Columbia. Annual reports pertaining to the top 10 Internet scams are available free of charge from the NFIC Website. Reports of Internet and online fraud have been launched by the NFIC since 1996.

Even though data was available from the respective annual IFW reports since 1996, this study only examined the period 1998 through 2002 because some of the crime categories in 1996 and 1997 were no longer on the top 10 lists provided from 1998 onwards. In addition, the data sets for two of the variables, payment methods used for committing the crime and demographic composition of the victims, were available only after 1998.

All the figures reported were in percentage and classified into the top 10 Internet scams. On any given year, the type of scam, their magnitude, and ranking on the list can be quite different. In some cases, the type of Internet scam may no longer be on the list after one or two appearances. New scams may also appear each year. From the period 1996 through 2002, there were nineteen types of online scam. When 1996 and 1997 were omitted for the purposes of consistency, there were fifteen types remaining.

Three processes were used for examining the data set pertaining to the type of Internet scams on the top ten listings. First, the percentages were sorted and the various scams were ranked. A "1"

was assigned to the scam with the highest percentage and a "10" was given to the category with the lowest percentage. Second, the numbers of occurrences on the top 10 lists were then tabulated. Third, if the Internet scam was found to occur in all five years, an average was then computed. The objective here was to identify those Internet scams that were most common and are still in use by con artists.

The two other variables, payment methods used for committing the fraud and demographics of affected persons, were examined using the same two statistical measures, the arithmetic mean and standard deviation. In addition, the raw data was also presented in tabular form. The objective in the latter two cases was to examine the raw data set for possible trends.

FINDINGS

Nineteen types of Internet scams or fraud were found among the seven top 10 listings obtained from 1996 through 2002. Four of those scams were no longer found on the top 10 listings after 1998 so they were removed from further analysis. They were (a) book sales, (b) club-membership or buyer's club, (c) investments, and (d) scholarship services. All four categories made the listings only once. With the exception of book sales that made the top listing in 1997, the other three were not found on the top 10 listings again after 1996.

Fifteen types of online fraud were found for the period 1998 through 2002. Six of the fifteen types of scams appeared to make the top 10 lists every year. Put in another way, some forty percent of the Internet scams appeared to be working very well or were very popular because they were consistently making the top 10 listings. Details about the respective types of online fraud are presented in Table 1 and discussed below:

- Auction fraud first appeared as the third highest category of online scam in 1997. Since 1998, it has consistently taken the number one place on the annual listings.
- Like auction frauds, the sale of general merchandise first appeared in 1997 as the second highest type of online scam. It has held on to this ranking ever since.
- In sequential order based on the average ranking over the five years, the other four categories that have made the top 10 listing are (a) sales of Internet services, (b) sales of computer equipment or software, (c) work-at-home, and (d) advance fee loans.
- One type of new Internet scam deserves attention. The Nigerian money offers made the top 10 listing in 2000 as the seventh highest ranked Internet scam. Since then, this category has climbed to the number three position in the most recent two years.
- The only other noteworthy scam category is adult services. It has made the top 10 listings since 1999 and appears to have consistently ranked between the 6th and 8th highest type of Internet scam.

Category of Internet Fraud	Year					Years of Occurrences	Average	Overall Rank
	1998	1999	2000	2001	2002			
Adult Services	N/A	8	8	6	7	4		
Advance Fee Loans	9	6	5	8	9	5	7.40	6
Auctions	1	1	1	1	1	5	1.00	1
Business Opportunities	6	N/A	N/A	10	N/A	2		
Credit Card Offers	8	N/A	9	9	N/A	3		
Job Offer/Overseas Work	10	N/A	N/A	N/A	N/A	1		
Magazine Subscriptions	N/A	7	N/A	N/A	N/A	1		
Nigerian Money Offers	N/A	N/A	7	3	3	3		
Prizes and Sweepstakes	N/A	N/A	N/A	N/A	10	1		
Pyramid Schemes/Multi-Level Marketing	7	10	N/A	N/A	N/A	2		
Sales of Computer Equipment/Software	3	4	6	4	4	5	4.20	4
Sales of General Merchandise	2	2	2	2	2	5	2.00	2
Sales of Internet Services	4	3	3	5	5	5	4.00	3
Travel/Vacations	N/A	9	10	N/A	8	3		
Work-at-Home	5	5	4	7	6	5	5.40	5

Table 1: Top 10 Internet fraud categories - 1998 through 2002

Category of Payment Method	1998	1999	2000	2001	2002	Average	Standard Deviation
Bank Debit	2%	1%	3%	5%	6%	3%	0.0207
Cash	3%	1%	3%	3%	2%	2%	0.0089
Cashier's Check	4%	5%	6%	4%	3%	4%	0.0114
Check	43%	39%	30%	18%	14%	29%	0.1268
Credit Card	8%	5%	11%	29%	34%	17%	0.1316
Debit Card	0%	1%	2%	6%	7%	3%	0.0311
Money Order	38%	46%	43%	30%	30%	37%	0.0733
Telephone Bill	1%	1%	1%	0%	0%	1%	0.0055
Trade	0%	1%	1%	0%	0%	0%	0.0055
Wire Transfer	0%	0%	0%	3%	1%	1%	0.0130
Others	1%	0%	0%	2%	3%	1%	0.0130
Total	100%	100%	100%	100%	100%		

Table 2: Internet fraud payment methods - 1998 through 2002

Online con artists were found to use some eleven types of payment methods to perpetuate Internet crimes. Using the five-year averages, it was found that there were three primary or

dominating methods namely, money order, checks, and credit cards. Several trends are worth discussing below:

- Even though checks have consistently been a top 10 payment method for Internet scams since 1998, the popularity of this media is showing a decreasing trend. In 1998, some 43 percent of the scams involved checks. By 2002, it had dropped to about 14 percent. In other words, it has lost about 75 percent of its popularity in the last five years.
- Money order, at one point was used in some 46 percent of online fraud, has now dropped to about 30 percent in the most recent two years.
- Credit card appeared to have replaced checks and money order as the fastest growing medium for perpetuating online fraud. Since 1999, its popularity as measured using the percentage extracted appeared to have multiplied almost seven fold.
- Even though small in percentage, bank debit cards and debit cards are the other two payment methods with an increasing trend.

Age Category	1998	1999	2000	2001	2002	Average	Standard Deviation
Under 20	2%	3%	2%	4%	3%	3%	0.0084
20-29	16%	20%	20%	26%	25%	21%	0.0410
30-39	42%	30%	28%	28%	28%	31%	0.0610
40-49	24%	27%	29%	24%	25%	26%	0.0217
50-59	12%	15%	15%	13%	14%	14%	0.0130
60-69	3%	4%	5%	4%	4%	4%	0.0071
70 and Up	1%	1%	1%	1%	1%	1%	0.0000
Total	100%	100%	100%	100%	100%		

Table 3: Age distribution of Internet fraud victims - 1998 through 2002

The IFW Project uses a total of seven age groups as the primary demographic criteria for tracking Internet fraud victims. With the exception of the first and the last categories, the rest of the groups are complied in age intervals of ten. As can be seen in Table 3 above, there are four groups that showed double-digit percentages. Using the averages for the five-year period, the four groups accounted for about 92 percent of all Internet fraud victims. About 78 percent, or about one out of every eight victims, was from the 20 through 49 age group categories. The highest affected group, about one out of every three victims, was from the 30-39 age group. Two major observations about the data set are discussed below:

- The 30-39 age group appeared to have plateau to about 28 percent, about one out of every three victims, since 1999.
- The 20-29 age group appeared to have picked up the drop in percentages from the 30-39 age group. In 1998, this group accounted for less than one out of every five victims reported. In 2002, this group grew to one out of every four victims affected.
- The 40-49 and the 50-59 age group categories appeared to be the most consistent group. In the case of the former, about one out of every four victims was from this age group. In the case of the latter, they accounted for one out of every six victims.

CONCLUSIONS AND MAJOR IMPLICATIONS

Using the publicly available NFIC data sets covering the period 1998 through 2002 in particular, this study found that there are certain trends and observations about online scams. First, six types of scams were consistently on the top 10 annual listings. During the period studied, Internet auctions and sale of general merchandise were the two most popular scams used by online con artists. The Nigerian money offers that have shown up on the top 10 list just three years ago is one online scam category that should be closely monitored. In any given year, certain new scams may also appear and existing ones may just drop off the list. However, the six online frauds that have made the listings all five years are expected to last for a while.

Second, the three most popular methods of payment used in Internet fraud are checks, money orders, and credit cards. Checks are declining in popularity as a fraud medium. Credit cards, on the other hand, are showing a steady increase as a medium for online scams. Even though a small percentage of the fraud involved only debit cards and bank debits, both these medium showed a slow but gradual increase.

Finally, based on the age groups used by the NFIC, victims of Internet fraud can be quite diverse. They range from those in the below 20 age group to those that are in the over 70 age group. However, some 92 percent of the victims are within the 20 to the 59 age groups. Over 50 percent of the victims are from the 20 to 39 age groups.

All the major trends obtained above indicate that computing educators can help to minimize Internet fraud in a variety of ways. First and foremost, one of every two victims of Internet fraud is from the two major age groups attending college. In a typical university, most of the traditional students are in the 20-29 age group and the non-traditional students are in the 30-39 age group. Computing educators can make a major contribution to the struggle against Internet fraud by educating these two groups of students about proper online shopping behavior. Ideal courses for covering this material may include but not limited to the computer literacy course in the general studies core, the information systems principles course or an introductory computer science course. With some understanding about what and how online fraud is perpetuated on the Internet, students will at least know what to watch out for when shopping on the Net. Since these courses are required of almost every student, this is one area where computing educators can provide the greatest impact.

Second, educating students about "right and wrong" decisions and the teaching of ethics should be included as a course in the undergraduate general core curriculum. Increasingly, universities have shunned away from the teaching of proper conduct and character building because often it involves the discussion about religion and value systems. Without a strong conviction, a highly competent and technology savvy graduate may become a liability to society by engaging in online fraud. A course in ethics can provide the needed education to a student to master what actions are acceptable and their limitations.

Third, computing educators can also help to minimize the Internet fraud problem by developing and designing courses on e-commerce security systems. Some of the technologies that have been included in recent course content include public key infrastructure, digital certificate and

authentication, information assurance, systems tolerance, and Web content analysis. Students who have taken courses in such cutting edge technologies will have the ability to build more secure computer systems.

Finally, computing educators can make a difference in the struggle against Internet fraud by providing the needed leadership for the creation of a multi-disciplinary major that can deliver secured systems for the new millennium. For example, computing educators can definitely team up with finance and accounting educators to identify potential payment systems that contain some form of intelligence for triggering real-time fraud warnings. A possible hinterland for such research funding may come from the banking industry because an overwhelming amount of the fraud is committed via the electronic money clearing system. Efforts toward the elimination or minimization of money losses should be of interest to the banking sector.

CAVEATS

There is at least one major limitation to the findings in this research. The trends identified are based on quantifiable cases reported in the NFIC reports. Individuals that have incurred a loss but have not reported them to the NFIC are not captured in the findings. If the proportions of unreported cases are significant, it could have affected the trends identified. It should be pointed out that major efforts were made to ensure that the outcomes are not compromised. The data set used was a reputable one and the method used for analyzing the data was robust. Great caution was also taken in interpreting the results.

REFERENCES

Associated Press (2003). Internet Fraud Has Tripled in One Year. *The Commercial Appeal*, A19.

Bennet, Madeline (2003). Internet Week - Service Guards Logos Online. *VNU Business Publications Ltd*, 23.

DeVeaux, P. (1999). Cache me if you can. *America's Network*, Vol.103, pp. 34-36.

Internet Fraud Watch. (1997). Keeping an Eye on Internet Fraud. Available at: http://www.fraud.org/internet/97.stat.htm.

Laurent, Belsie (1997). Two best defenses against online fraud: caution and credit. *Christian Science Monitor*, 89(204), 15.

Lee, W. A. (2003). Progress Report from BITS on Fraud Prevention Effort. *The American Banker*, 1.

Manuel, Cleo (1999 February). Internet Fraud Watch. Available at: http://www.fraud.org./internet/9923stat.htm.

PBI Media (2003). Taking a Bite out of Financial Fraud. *PBI Media, LLC*, 14(4), 1-6.

Petska, K. (2001). 625 Million Computers in Use Year Ended 2001. Available at: *http://www.c-i-a.com/200107cu.htm*.

Theel, T., Stephens, G., and Easland M. (2001). Demand it. *Satellite Communications*, 24, 26-31.

Trebilcock, Bob (1998). Don't Get Scammed on the Internet. *Good Housekeeping*, 227(2), 161-163.

U. S. Department of Justice (2003). Internet Fraud. Available at: http://www.internetfraud.usdoj.gov

U. S. Federal Trade Commission - Bureau of Consumer Protection (2003). Internet Sparks Growing Consumer Fraud Complaints, *Washington Internet Daily*, 4(15), 1-2.