The Bill Blackwood
Law Enforcement Management Institute of Texas

===============

# Internet Fraud: The New Challenge to Law Enforcement of the Twenty First Century

===============

An Administrative Research Paper
Submitted in Partial Fulfillment
Of the Requirements for Graduation from the
Leadership Command College

===============

by
William E. Cole

Greenville Police Department
Greenville, Texas

January 2002

TABLE OF CONTENTS

Page

# ABSTRACT

Internet fraud is one of the fastest growing criminal offenses in the world, and the problem

is compounded by rapidly changing technology placing many law enforcement agencies at a severe disadvantage. All of the law enforcement agencies in the world are affected by this crime. Criminals around the world have proven that they can breach the secure web sites of the most powerful companies in the world, even the computer giant Microsoft is not safe.

Government officials, law enforcement and members of the business world have examined

the problem of Internet fraud. During the studies done by various groups several ideas for combating Internet fraud were proposed. Although several ways have been explored by law enforcement to deal with Internet fraud the overwhelming belief by those involved in the investigation of Internet fraud is that the solution is to educate the public in how to prevent the crime from occurring.

In addition to increasing the amount of information that is provided to the public about Internet fraud lawmakers need to address the obstacles that hinder law enforcement officials during the investigation of these types of offenses. Any changes in existing laws will need to be accompanied by a tremendous effort on the part of all concerned to over come the barriers of language, culture politics, and social values, which vary greatly in other countries.

Law enforcement must join with the business world if there is any hope to slow this rapidly growing crime. New friendships must be form between countries so that cooperation

between investigators can be achieved, and foremost the public must be informed of the dangerous of Internet fraud.

## INTRODUCTION

Internet fraud is a common occurrence, and has become perhaps the fastest growing crime in the world today. The educated criminal can now use a computer from anywhere in the world to victimize those who use the Internet. How is the public to protect themselves when criminals break into the most secure computers in the World? How do small police departments with limited resources investigate Internet crime? This research is intended to show the need for an International Task Force composed of Criminal Investigators along with new ways to help prevent criminals from victimizing Internet Users and the education of Internet Users.

Police officers today are faced with a new problem as we enter the Twenty First Century, which gets larger every day as the criminal element becomes more knowledgeable about computers. The explosion of the Internet a few years ago opened new doors for criminals. The use of computers to commit crimes has severely handicapped Law Enforcement as a whole. Police agencies with limited resources must rely on larger agencies to assist in the investigation of Internet crimes. Recently the Federal Bureau of Investigations (FBI) posted a new Web site, which allows a victim of Internet fraud to go on-line and make a complaint. The problem is the FBI then sends the complaint to the local police agency. Most of the time the actors in these offenses are migratory in nature, and with good reason. Since most small police agencies do not have specially trained investigators for Internet Fraud these cases are at a stand still. Most Federal Law Enforcement agencies will not get involved in an investigation for any type of fraud or theft unless the aggregated amount is $ 25,000.00 or more. The decision by the FBI and other federal agencies to investigate cases only after a certain threshold is reached is understood by local police.  Certainly the number of offenses makes investigation by these agencies an impossibility.  Most cases do not come close to $ 25,000.00, and if they do it is difficult to determine without help from an agency such as the FBI.

Thus the question is posed; how is Law Enforcement as a whole to deal with a problem that reaches to every corner of the world?   Many small police agencies that do not have specially trained personnel are at further disadvantage.  The solution will require a great deal of cooperation from the many different Law Enforcement agencies around the world, and the funds to meet this need.  The information contained within this writing will only address the need for such action.

This project will begin with an analysis of the literature available on Internet Fraud. The analysis will show how Internet Fraud has grown at an alarming rate in the past three years.  The research will also show how law enforcement and business are combating Internet Fraud at present.    The analysis will include interviews with law enforcement officials who are actively involved in the investigation of Internet fraud.

It is hypothesized that a multi-jurisdictional police unit will emerge in the future, which will be composed of local, state, and federal officers, who will work with police officers around the world to combat Internet Fraud.  This multi-jurisdictional unit will function in the same manner as many other Task Force Units formed to combat other crimes.   This hypothesis will be supported by current efforts now being employed by law enforcement.  The need for such a Task Force will be illustrated by documentation of the numerous crimes committed in the United States and around the world in the recent past.  This hypothesis will include the need for such a Task Force to work in cooperation with state and local governments to educate the public about Internet Fraud, and to encourage technological advancement to help prevent

Internet fraud.

If a multi-jurisdictional police unit is not eventually undertaken the Internet Fraud criminals of the world will have no reason to fear in certain areas of the world where this vision is not seen. Investigation into computer crimes is a complicated task, and without cooperation from other police agencies around the world the victims of such crime will continue to grow at an alarming rate. It is the hope of this writer that this vision will be seen by those who are in the position to implement the change necessary for investigation of Internet fraud around the world.

# REVIEW OF LITERATURE

On February 10, 1998 the Committee of Government Affairs subcommittee met to discuss fraud on the Internet and scams affecting consumers. Senator Collins addressed the subcommittee, and during his presentation he commented that the potential for use of the Internet by criminals is infinite. Senator Collins went on to say that fraud via the Internet had increased three hundred percent over the past year as documented by the National Fraud Information Center. Senator Collins also pointed out that criminals were quickly learning that almost any crime that could be committed could be committed on the Internet with much less chance of getting caught (1998).

The BBC News reported on April 7, 1999 that Internet fraud knows no borders. Citing the United States as the leader in Internet use as well as misuse, the BBC News referenced a report done by a U. S. company called Cyveillance. In the report the results of a study of 150,000 web sites researched indicated that about 20,000 to 25,000 of the web sites are scamming consumers using phony merchandise. Another concern was copycat web sites in which merchants are tricked into thinking they are dealing with a well-known company.

According to Visa International (1999) half of all disputes about credit card charges made stem from the Internet. This statistic is staggering when only about two percent of Visa's business is from on-line purchases. A large number of the disputed charges are made with stolen credit card numbers. In yet another scam financial were targeted across the United States where the Internet was used to sell life insurance to individuals with life threatening illnesses. About one hundred million was lost to the scam artist. Another point brought to light during the research of this project is that businesses and financial institutions cover up many scams because they do not want to cause panic among consumers and investors.

James G. Huse Jr. the Inspector General for the Social Security Administration addressed the subcommittee for the Committee on Governmental Affairs on the May 19, 2000 concerning the use of the Internet to commit fraud. Mr. Huse reported to the members of the subcommittee that obtaining fraudulent social security cards over the Internet had become a very large problem for his office. Mr. Huse also pointed out that use of the fraudulent social security cards lead to other crimes such as credit card fraud. Mr. Huse described the impact to the economy as staggering. It should be considered that since Mr. Huse spoke about this topic in May of 2000 the use of Internet services has grown tremendously as have the number of criminals who prey on the unwary consumer.

In a statement made by Senator Ron Wyden o March 15, 2000 to the United States Special Committee on Aging, Senator Wyden reported that telemarketing and cyber fraud were costing the citizens of the United States 40 billion each year. The average loss to each senior citizen victim was between $ 5,000 and $ 20,000 dollars.

On May 19, 2000 Senator Collins again address the subcommittee of the Committee on the Governmental Affairs. Senator Collins statement was in response to the ease at which criminals could obtain fraudulent identification over the Internet. In the address it was pointed out that virtually any form of identification could be obtained using the technology available from the Internet including identification of FBI and CIA agents. Using the technology from the Internet and a few arts and crafts supplies anyone could produce the fake identifications according to Senator Collins. It was also pointed out that even the security features used by state agencies and credit card companies were offered on the Internet. During the investigation it was discovered that one Internet web site operator had sold about 1,000 fake identifications each month with an annual income of about $ 600,000.  At least one of the web sites offered fake utility bills to help individuals pass themselves off as the person whose identity they had assumed.  The fake identifications obtained are frequently used to commit other crimes, and are considered essential for committing financial crimes.

The information that can be found on the Internet includes bank account numbers, credit card numbers, and even secret business secrets.  With an explosion in the use of the Internet intrusions have become all too common.  Even Microsoft is not safe.  In light of such threats to security, training seminars have began all across the country.  San Jose Federal Bureau of Investigations agent Dave Townsend who is assigned t the Rapid Enforcement Allied Computer Team warns that computer crime will just get worse.  Agent Townsend has to spend about one week each month in training just to try to keep up with the changes in technology and the criminals.  The need for computer specialist in law enforcement is upon us, and even small departments may find themselves faced with assigning an investigator to handle computer crimes (Corkery, 2000).

On May 23, 2001 the Committee on Energy and Commerce heard testimony from agents on the Secret Service concerning the ability of criminals to commit crime over the Internet using false identification.  The information in the statement to the committee was redundant in that there seems to be little progress made by law enforcement to curtail Internet fraud.  Bruce Townsend who spoke to the committee did conclude his statement by saying the Secret Service would continue to work with both domestic and global law enforcement partners in fighting Internet fraud.

A study funded by the National Institute of Justice in 1998 to look for ways to solve the problem of Internet investigation was perhaps one of the most in-depth looks at how to combat Internet fraud since the inception. The study yielded two mayor points and ten critical needs. The points stress were the need for immediate high-ended computer forensic training or to assemble task forces. What was agreed upon was the need to progress quickly in a combined effort. The ten critical needs were not given any certain priorities. Public education and law enforcement training seemed to stand out among the ten critical needs. The conclusion that this study provided was that Local, State, and Federal authorities should get involved before the criminal element is beyond reach. The Internet knows no boundaries yet law enforcement generally is restrained by jurisdictional limitations. Training and technological advancement should be immediately undertaken along with future study of the problem (Stambaugh, et.al.2000).

Online fraud committed through auction web sites ranked number one two years in a row as documented by the Federal Trade Commission. The FBI reported that only one percent of the transactions made on auction web sites resulted in fraud, but the FBI also stated that there were over 4,000 complaints made in the first four months of 2001. Local agencies are starting to assemble special units to deal with the problem. In Akron Ohio a special Internet fraud unit was assembled between the FBI and Summit County Sheriff's. Akron Police Detective Stanley Smith describes Internet crime as a global problem (Soenarie, 2001).

The results of on line fraud are higher credit card fees due to the business of dealing with unstable companies using the Internet, and customers whose identities are often impossible to prove. A good example of this is a recent scam in which European thieves invaded U. S. merchants web sites using stolen credit card numbers. This tactic was also used to buy a form of on line currency called flooz, which is essentially like cash to spend on the Internet. The result was bankruptcy for the company flooz.com (Tedeschi, 2001).

Teams of prosecutors and investigators working together have been organized to fight computer crime according to U. S. Attorney General John Ashcroft. The teams will focus on intrusions, thefts of trade secrets, copyright and trademark thefts, and economic espionage. In a survey done by the FBI it was discovered that about 85 percent of government agencies and businesses have discovered computer breaches n the past year. The study also noted that U. S. businesses have spent 300 billion in the past year fighting fraud (Sebastian, 2001).

Visa has announced a new security device called Visa Payer Authentication, which allows for safer use of the Internet for both the merchant and consumer. Using advanced technology the device will act as a security wall between consumers and merchants to verify identities thus allowing for safer on line shopping, electronic transactions, and other information traveling over the Internet.

The U. S. Congress Committee on Energy and Commerce subcommittee heard testimony from the Federal Trade Commission's (FTC) Eileen Harrington about the rise in Internet fraud, and how the database used by the FTC (Consumer Sentinel) was an effective tool in the investigation of Internet fraud. Mr. Harrington also pointed out that because of the pace, which e-commerce was moving world wide, new relationships with other law enforcement counter parts in other countries must be established to fight Internet fraud. The FTC has undertaken this task by establishing relationships with other countries through the International Marketing Supervision Network, a network with 30 other member countries. Another association the FTC has joined is the Organization for Economic Cooperation and Development (OECD). This project fosters relationships in law enforcement with other member countries, and provides for online complaint forms in various languages.  The OECD provides for two web sites, a public web site for complaints and a restricted web site for law enforcement.  The combination of these web sites will provide investigator with another tool with which t fight Internet fraud.

One clear method of preventing fraud over the Internet is using technological advancements such as new software recently implemented by Safeco called Netmap by Alta Analytics.  The software uncovered a scam by two doctors who were no longer practicing medicine, but continued to make fraudulent claims against Safeco (Institute of Management & Administration, 2001).

The Federal Trade Commission (FTC) teamed up with law enforcement officer from nine countries and twenty-three states to file 251 charges against online scammers, web auctions topped the list.  Jodie Burnstein, the FTC's Bureau of Consumer Protection, wants all cyber criminals to know that the FTC is building a coalition throughout the world with which to make using the Internet a sage place to do business.  The FTC also met with the International Marketing Supervision Network, which includes consumer enforcement protection authorities from 29 countries.  The FTC acknowledges they want to boost international cooperation to protect consumers (Federal Trade Commission, 2000).

On line consumers lost one million more dollars in the first ten months of 2001 compared to all of 2000.  Web auctions remained at the top of Internet fraud complaints, but decreased 15 percent from the previous year.   There is obviously a need for more education and enforcement if this trend is to be slowed.

In Paris France there is a school taught to those who wish to learn how to hack.  The instructor, a teenager going by the name Clad Strife, claims he only teaches what he refers to as good pirate skills.  The students claim their interest to be only one of self-defense against other hacker (Coomarasamy, 2000). Obviously anyone could attend this type of training, which could be used for either good or bad.

Within hours of the World Trade Center tragedy on September 11, 2001 the scams began. There were fraudulent e-mails asking for donations, and phony web sites asking for donations for the fallen. Some of the con artist posed as public servants playing on the public's sympathy for the police officers and fire fighters killed during the catastrophe (Mannix, 2001). This practice occurs on a day-to-day basis with current events playing a role on the type of angle used by the crooks.

Four teenagers were arrested in Jerusalem for creating and causing the computer virus "Goner" to spread over the Internet to hundreds of users. There were more than 400 attacks of the virus reported by American anti-virus companies in the world (Copans, 2001). This practice seems to be popular among Americans as well. It is all too common for e-mails to include some type of computer virus.

The Securities and Exchange Commission (SEC) says a 17-year-old high school student masterminded a scam, which cheated about 1,000 investors out of more than a million dollars during a two-month period. Education seems to be the best thing the SEC can do for the public at present as apprehension of on line scam artist is very difficult (Weisman, 2002)

Identity theft was counted for forty two percent of the complaints made to the Federal Trade Commission (FTC) for the year 2001. The FTC maintains that a large amount of the identity theft is related to Internet fraud. Although the static's indicate that Internet fraud double during the year from the previous year large part is due to the increased efficiency of the reporting system using on line complaint forms available to the public. This explains in part the alarming statistics the press had blown out of proportion.

# METHODOLOGY

This research project is intended to show the need for an international task force along with increased public education about Internet fraud and the new ways to prevent criminals from committing Internet fraud.

When considering all of the obstacles for law enforcement to deal with at present it is believed that public education is the most cost efficient way to deal with the problem of Internet fraud at present;  however law enforcement must work with those who specialize in the technology needed to investigate Internet fraud.  Law enforcement must continue to educate them about the technique used to investigate Internet fraud as it is a ever-changing process. Law enforcement must also foster new relationships with authorities in other places around the world as Internet fraud is a global problem, which threatens all people who use the Internet or have personal information, which can be accessed by the Internet.  Law enforcement needs the assistance of lawmakers to make new laws, or change and modify laws as needed to ensure law enforcement has the tools necessary to investigate Internet fraud.

The primary method of inquiry for this research is the review of literature available on the subject along with personal interviews conducted with law enforcement authorities currently involved in Internet investigations.  The interviews were done with local, state, and federal officers in hopes of getting a wide variety of views on the problem.

The instrument used to gather information was completed by e-mail in which the Internet investigator was asked to list the following topics in order as which was considered the best way to combat Internet fraud in their opinion.   The topics were compiled from the information covered in the review of literature.

Public education

Technology

Training law enforcement in computer skills

Creation of a international task force

Other- please list idea(s)

The investigators were then asked to give their opinion about Internet crime from a global perspective, and what needs to be done by law enforcement to deal with the problem.  Responses were obtained from two investigators in large departments that being the Dallas Police and Austin Police Departments.  A response was also obtained from a Postal Inspector and a Secret Service agent.  A request was also made to the Texas Attorney Generals Office, but no response was received.  A comparison of the answers from each of the Internet investigators was made to draw a conclusion.

# FINDINGS

When looking at the Internet from a global perspective and the news of how criminals around the world are exploiting the use of the Internet if becomes a problem which law enforcement cannot deal with using the current technology and training.  There is obviously a need for progress in the way Internet crime is investigated from a global perspective, but there are other ways in the immediate future that Internet fraud can be combated.

The statistics continue to climb at an alarming rate as more and more individuals become Internet users.  This problem will only get worse until somehow the public is educated on how to protect themselves when using the Internet; however a few basic safety rules for Internet use would make using the Internet to shop a much safer place.

The literature covered in this project all has one common denominator that being education of the Internet users.  If all Internet users were fully aware of the potential for becoming victims of Internet fraud the who perpetrate these crimes would not have much success.  There have been many inquiries into how to deal with Internet fraud. Law enforcement has made some progress and there have been some areas identified in which improvement needs to be made.  The most needed area is training, but even training cannot accomplish what education of the public could do in preventing the crime from occurring.  If a person were to simply read about the use of the Internet much in the same way any inquiry would be made they would find a wealth of information about Internet fraud and how to prevent fraud and report Internet crime.

Lawmakers should join in with law enforcement officers by amending laws or changing them so that criminals can be brought to justice.  This issue will not be solved in the near future as civil rights protect many criminals.  In some countries what is crime here is legal there, and what is crime there is legal here.  This problem is less likely to be solved than the issue of civil rights and the protection of information by Internet provider who are very reluctant to release information about uses.  Internet providers commonly ignore legal subpoenas for information stating they will only comply with a search warrant.  This lack of cooperation and the part of Internet providers handicaps law enforcement.  Lawmakers should amend laws so that Internet providers are forced to comply wit legal subpoenas rather than forcing law enforcement to spend numerous hours writing search warrants for information needed to prosecute crime.

Technology is certainly a good tool to help combat Internet crime, but like any lock it can be defeated if a person takes the time.  When you consider that 85 percent of all government agencies and businesses have been victimized by some type of computer breech in the past year coupled with the billions of dollars spent to try to prevent computer crimes it is obvious that technology alone is not going to fix the problem.  Technology is a good tool for fighting Internet fraud and should be continually developed in conjunction with other ways to fight the problem.  The largest corporations have been victims of computer hackers.  Often vital information is compromised or stolen.  Many times the results are massive credit card abuse or loss of trade secrets.  No matter what the loss technology must be accompanied by competent investigations in which relentless investigators and prosecutors trained in this type of crime to bring those guilty to justice.

There are many countries working together to investigate Internet fraud schemes around the world.  Law enforcement has enjoyed some success in bringing some criminals to justice for certain crimes.  The Federal Trade Commission, Federal Bureau Of Investigations, Secret Service and many other United States agencies have worked with other countries to find and prosecute criminals in other countries.  The efforts put forth by these agencies commendable. The participation of United States law enforcement with other countries could be the making of a global task force to fight Internet fraud, but at present there are far to many differences in the laws of other countries and the lack of cooperation of others.  For now the world will have to be content with a few battles won in the war of Internet crime.

According to the Internet investigators who were contacted and responded t the questions posed to them they were evenly split on public education and training for law enforcement as the two most important ways to fight Internet fraud.  Changes in laws to aid investigators was third followed by technology.  The need for an international task force was last in the listing by the investigators even though it is partially a reality at present.  When asked what their opinion was about Internet fraud from a global perspective, and how to deal with it the response was much the same from all. The same opinion seemed to come from all of the investigators in that there are far to many differences in other countries for the United States to get complete cooperation in investigation into Internet fraud.  Tim Allen of the Secret Service stated that he had been assigned twice to Nigeria in the last two years.   On both occasions Tim was sent there to investigate fraud schemes that victimized United States citizens.   Tim encountered police stations that did not have electricity, much less computers.   Computers that had been seized were stored in outside property pens unprotected from the elements.   Needless to say they no longer had any evidentiary value.   The police in Nigeria have trouble even understanding what computers are according to Tim.  Some of the equipment seized by the Nigerian police had been outside for two years says Tim.  In Romania there is a problem with on line auction fraud.  This problem gets very little attention according to Tim when the country is overwhelmed by violent crime.  The United States sends financial aid to some of the countries to help assist them in investigating Internet crimes against the United States, but just enough is done to ensure that the financial aid will keep coming.

# DISCUSSION/CONCLUSIONS

Law enforcement officials around the world are faced with a tremendous problem in combating Internet fraud from a global perspective. This project is meant to inquire into the possible ways to provide viable solutions to this very complicated issue. This research also poses the question, is an international task force assembled to fight Internet crime a possibility?

The theory behind this project is that an Internet task force made up of law enforcement officials around the world is needed to investigate Internet crime because of the ease at which criminals around the world commit Internet fraud. The sources used in this research indicate that some law enforcement officials around the world are working together to fight Internet crime. There are so many factors to deal with as in any matter concerning other countries. Language, culture, politics, social values and many other issues will prevent the realization of such a special law enforcement unit from ever becoming a reality. Certainly many criminals will be brought to justice by some countries working together, but for now other means must be used t fight the problem.

The information found in the research seems to indicate that several avenues should be pursued in the war on Internet fraud. The first and most vital need is to educate the Internet user about Internet crime and how to avoid it. The education of the public must be accompanied by skilled investigators trained in the tactics needed to investigate Internet crime, and accompanied by specialist in computer knowledge. The next step is to ask computer software makers to continue to strive to make better software capable of keeping information safe from hackers, and also identifying computer attacks so that hackers can be tracked down. The creation of an international task force ranks last in the order of things immediately necessary to fight Internet crime. The literature covered in this project documents that the United States of America is the leading user of Internet services in the world. As such Americans commit most of the crime committed against Americans. If another country does attack the United States through the Internet a response will follow. That problem has occurred and the results have been technology designed to prevent future attacks such as hacking into credit card companies files.

This research does not include opinions of officials from around the world although some of the literature does come from other countries where law enforcement officials from other countries voice their opinions. Most of the literature comes from the American perspective, which is likely to be less than popular in other places, and that is the problem with most all other issues between countries. The investigators questioned via e-mail confirmed the point made in the review of the literature in that education is the number one answer to the problem.

This research covers a new topic which is rapidly changing in a fast pace environment. The investigators who undertake this field of investigation need to be prepared to change with the times and be willing to constantly train to stay abreast of the criminals who feed on the ignorance of the common Internet user. Law enforcement must reach out and make new friends who have the skills needed to assist them in the investigation of Internet fraud, and prosecutors must prepare themselves for the complicated task of prosecuting these crimes.

# REFERENCES

BBC News, (1999 April, 7) Business: Your Money Fighting on-line fraud [on line]. Available: http://news.bbc.co.uk/hi/english/business/your_money/newsid_312000/312718.stm.

Coomarasamy, J. (2001, December, 1) Learning to hack, BBC NEWS [on line]. Available: http: //news.bbc.co.uk/hi/english/world/Europe/newsid.

Copans, L. (2001) Israli teens admit unleashing computer worm attack, Nando Times [on line]. Available: wysiwyg://91/http://www.nando.net/technology/story/1901175p-1841930c.html.

Corkery, J. (2000) Careers in Hi-Tech Security: Collaring the Cybercrooks. California Job Journal [on line]. Available: http://www.jobjournal.com/article_full_text.asp?artid=63.

Elder fraud and abuse: New Challenges in the Digital Economy, One Hundred Sixth Cong., Second Sess. (March 15, 2000).

Federal Trade Commission, (2000, October 31) Law Enforcers Target "Top 10" On Line Scams [on line]. Available: **http://www.ftc.gov/opa/2000/10/topten.htm.**

Financial Times Information (2001, September 7) Costa Rica-Fraud two U.S. Citizens arrested in Costa Rica for Internet Fraud [on line]. **Available: http://web.lexis-nexis.com/universe/document.**

Fraud on the Internet: Scam Affecting Consumers, One Hundred Fifth Cong., Second Sess. (February 10, 1998).

Getzfred, M. S. (2001, July 25) Technology Briefing Internet: Web Site Selling Id's Settles, The New York Times, Sec. C; p. 4; Col.3.

Hearing on the Sale of False Identification Documents Via the Internet, Committee on Governmental Affairs Permanent Subcommittee on Investigations, U. S. Senate (May 19, 2000).

Institute of Management & Administration, (2001) Preventing Business Fraud [on line]. Available: http: //web.lexis-nexis.com/universe/document.

Lyman, J. (2002, January 23) ID Theft and Web Scams Top Consumer Complaints, YAHOO!NEWS [on line]. Available: wysiwyg://23/http://dailynews.yahoo.com.

Nando Times (2001) Technology: Israeli teens admit unleashing computer worm attack [on line]. wysiwyg://91/http://www.nando.net/technology/story/1901175p-1841930c.html.

Mannix, M. (2001) Cashing in on Fear. U. S. News & World Report, Vol 131 (issue 23), p. 36.

On-line fraud and crime: Are consumers safe?, One Hundred Seventh Cong. , First Sess. (May 23, 2001).

Phony ID's and Credentials Via the Internet: An Emerging Problem, One Hundred Sixth Cong. , Second Sess. (March 15, 2000).

Prentice Hall Law & Business (2001 August) FTC Testifies that E-Commerce is Fertile Ground for Fraud [on line]. Available**: http://web.lexis-nexis.com/universe/document.**

PR Newswire Association, Inc. , (2001,July 30) Cardinal Commerce Selected by Visa U. S. A. as a Vendor for the Visa Payer Authentication Service [on line]. Available: http://web.lexis-nexis.com/universe/document.

PR Newswire Association, Inc. (2001, August 14) Clear Commerce Announces tips to Protect Consumers from On-Line Fraud This Holiday Season [on line]. Available: http://web.lexis-nexis.com/universe/document.

Sebastian, M. (2001, July 21). Attorney General unveils new Federal initiative to fight Web Crime. Knight Ridder/Tribune Business News, Contra Costa Times.

Soenarie, A. (2001, August 26). Internet Fraud Increases as More People Go On-Line. Akron Beacon Journal.

Spamming, One Hundred Fifth Cong., Second Sess. (June 17, 1998).

Stambaugh, H. , Beaupre, D. , Icove, D. J. , Baker, R. , Cassaday, W. , & Williams, W. P. (August 2000). State and Local Law Enforcement needs to combat electronic Crime. National Institute of Justice, 1-6.

U. S. News & World Report (2001 December 3), Vol. 131 issue 23 p. 36 Cashing in on Fear [on line]. Available: http://web.lexis-nexis.com/universe/document.

Weisman, R. (2002, January 8) U. S. Teen Behind $ 1M Internet Fraud Scheme, YAHOO!NEWS [on line]. Available: wysiwyg://34/http://dailynews.yahoo.com.