The Growing Global Threat of Economic and Cyber Crime

The National Fraud Center, Inc.
A member of the Lexis-Nexis Risk Solutions Group

In conjunction with
The Economic Crime Investigation Institute
Utica College

TABLE OF CONTENTS

I. Introduction 5
II. Executive Summary
- Traditional & Cyber Economic Crimes..... 6
  - Banking..... 6
  - Credit Card..... 7
  - Health Care..... 7
  - Insurance..... 7
  - Securities..... 8
  - Telecommunications..... 8
  - Intellectual Property & Computer Crime..... 9
  - Identity Theft..... 9
- Impact of Technology on Economic Crime..... 9
- Global Implications for Economic Crime..... 10
- Future Needs and Recommendations..... 10
- Conclusion..... 11

III. Growth of Economic Crime
- Economic Crime Defined..... 12
- Types of Economic Crime and Statutory Law..... 13
  - Mail & Wire Fraud: Generic Frauds & Swindles..... 13
  - Banking Industry: Financial Institution Crimes..... 14
  - Credit Card Crimes..... 15
  - Health Care Fraud..... 16
  - Insurance Fraud..... 17
  - Securities Fraud..... 17
  - Telecommunications Fraud..... 18
  - Intellectual Property and Computer Crime..... 19
  - Identity Theft..... 20

IV. Impact of Technology on Economic Crime
- Banking..... 22
- Credit Card..... 23
- Health Care..... 23
- Insurance..... 24
- Securities..... 24
- Telecommunications..... 24
- Intellectual Property & Computer Crime..... 25

V. Victims of Economic Crime

Consumers…….. 28
Industry……. 28
Government……. 29
VI. Waging the War on Economic Crime
Law Enforcement……. 31
National Fraud Center……. 31
Economic Crime Investigation Institute……. 32
National White Collar Crime Center……. 32
National Coalition for the Prevention of Economic Crime…… 33
Internet Fraud Council……. 33
Internet Fraud Complaint Center…….. 33
Independent Corporations and Private Sector Industry Coalitions…….. 34
VII. Future Needs and Challenges
Law Enforcement Training……. 35
Laws, Regulations and Reporting Systems……. 35
Public-Private Partnerships……... 36
Balancing Privacy Interests……... 36
Global Interaction and Cooperation……. 38
VIII. Conclusion: Trends and Observations…….. 40

IX. Statistic Matrix……. Appendix 1

Forward

The National Fraud Center as part of its mission, continues to research, analyze, and combat economic crime. Its focus and expertise on economic crime has continued for over 18 years. While seeing dramatic change and growth in economic crime over the years, it is increasingly evident that there are consistent, underlying fundamental issues that need to be addressed. The rapid growth of technology, as well as increased competition, has helped fuel the dramatic rise and cost of economic crime; therefore exploiting the weaknesses and challenges we as a nation, business, and consumer face. This report is the National Fraud Center's continuing contribution to assisting in eradicating this growing epidemic. We as a global society have many complex challenges ahead. We believe this report will continue to educate and stimulate the ability for dramatic change in researching, preventing, and investigating economic crime.

About the Authors

This report was supported and directed by National Fraud Center, Inc. (NFC). It was written by Dr. Gary R. Gordon and Dr. George E. Curtis, with directional and expert support from Mr. Norman A. Willox, Jr., and technical and research support from the staff of NFC, lead by Greg Peckham. Dr. Gordon is Executive Director of the Economic Crime Investigation Institute, as well as Vice President of Cyber Forensics Technology for WetStone Technologies, and a full professor at Utica College. Dr. Curtis is the Director of Economic Crime Programs at Utica College, where he is an Associate Professor. Mr. Willox is the Chairman of the Board of NFC and Director of Government Relations for Lexis-Nexis Risk Solutions Group.

The National Fraud Center, Inc. (NFC) is a recognized leader in fraud and high-risk solutions, providing expert consulting, best-practices, product reviews and solutions support. NFC is a wholly owned subsidiary of Lexis-Nexis, and part of the Lexis-Nexis Risk Solutions Group. Lexis-Nexis Risk Solutions Group is the nations leading provider of fraud and risk management information solutions for industry and government. Lexis-Nexis Group is a Reed-Elsevier PC Company.

Peer Review

Peer review of this report was conducted by executives of the National White Collar Crime Center (NW3C) and the National Coalition for the Prevention of Economic Crime (NCPEC), lead by Richard Johnston and Allan Trosclair. Mr. Johnston currently serves as the Director of the NW3C. Mr. Trosclair is the Executive Director of the NCPEC.

I. Introduction

The purpose of this report is two-fold: 1. To present an assessment of the state of economic crime in the United States, and; 2. Based on that assessment, to indicate areas where additional research, legislative action, training, cooperation between law enforcement and industry, and international cooperation are required.

Such a study is challenging, because of the paucity of reliable data. As is discussed in Section III, there is no central repository of statistical information on economic crimes. Available statistics and data were obtained from reliable sources including government agencies, industry associations, private sector organizations, Internet sites, and online databases, including Lexis®-Nexis®.

The data presented here provides the basis for a discussion on economic crime in the United States and clearly points out the challenges that will be faced in the near future.

II. Executive Summary

The American people have had contradictory views of economic crime for some time, seeing it either as a minor issue or a major crisis. In the past twenty years, there have been times when it has been in the limelight because of a financial crisis, e.g. the Savings and Loan Scandal and the insider trading problems in the 1980's. Usually, it has taken a back seat to a strong national focus on more conventional crimes, specifically violent ones. Many estimate the cost of economic crime to be over $500 billion annually.[1] There has been a significant increase in these figures over the past 30 years; in 1970 the cost was approximately $5 billion; it rose to about $20 billion in 1980, and approximately $100 billion in 1990.[2] As the Internet and technological advances continue to reshape the way we do business in government and industry, and competition and economic pressures create quicker and more efficient ways to do business, the reality of increased economic crime having a serious impact on the economy grows geometrically.

All the financial segments of the United States economy report significant losses as a result of economic and computer crime. This report provides the latest and most reliable statistics in eight key areas: banking, credit card, health care, insurance, securities, telecommunications, intellectual property and computer crime, and identity theft.

TRADITIONAL AND CYBER ECONOMIC CRIMES

While some types of economic crime are specific to the seven areas of this report, other types, such as identity theft and false statements, cut across all industries. Traditional economic crimes and new cyber crimes are discussed in this report. Current statutory laws are discussed for the crimes within each of the eight areas discussed below.

Banking

Ernst & Young reports that more than 500 million checks are forged annually.[3] In 1997, the American Bankers Association reported that banks lost $512 million to check fraud.[4] *American Banker*, an industry magazine, predicts that there will be a 25% increase in check fraud over the next year.

Money laundering has increased over the last ten years. As a result, global efforts to combat this crime have increased. While it is extremely difficult to estimate the amount of worldwide money laundering, one model estimated that in 1998 it was near $2.85 trillion.[5]

The growth of online banking presents other opportunities for perpetrators of economic crime. Funds can be embezzled using wire transfer or account

takeover. “Customers” can submit fraudulent online applications for bank loans. Hackers are able to disrupt e-commerce by engaging in denial of service attacks and by compromising online banking payment systems. Identity takeover can also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions.[6]

Credit card

According to Meridien Research, estimated fraud loss for the credit card industry amount to $1.5 billion annually[7], of which $230 million is estimated to result from online transactions. MasterCard reported a 33.7% increase in worldwide fraud from 1998 to 1999. During the first quarter of 2000, fraud losses increased 35.3% over the last quarter in 1999. VISA reports similar trends. It is estimated that fraud losses for online transactions may exceed $500 million in 2000.[8] Fraudulent credit card activities include the use of counterfeit, stolen, and never-received cards, as well as account takeover, mail order and Internet card-not-present transactions.

Health care

Health care fraud includes frauds perpetrated upon government-sponsored and private health care benefit programs by insiders, the insured, and providers. Losses for 1999 were estimated to be about ten percent of all money spent on health care, which translates to a loss of approximately $100 billion. [9] Health care related cyber crimes include obtaining pharmaceuticals from Internet sites by providing false information and web sites that claim to provide expert medical advice, but, in fact, do not have any medical professional involved.

Insurance

According to an FBI report on insurance fraud, published on its web site under “The Economic Crimes Unit” section, total insurance industry fraud is 27.6 billion annually. The Coalition Against Insurance Fraud breaks the total down across the insurance industry as follows:

- Auto $12.3 billion
- Homeowners $1.8 billion
- Business/Commercial $12 billion
- Life/Disability $1.5 billion
    - Total $27.6 billion[10]

Economic crimes in this area include those committed both internally and externally. Internal fraud can manifest itself in bribery of company officials, misrepresentation of company information for personal gain, and the like.

Applicants, policyholders, third party claimants, or agents providing service to claimants can commit external fraud. The fraud can take the form of inflated claims, false applications resulting in the issuance of fraudulent policies, or manipulating information in order to lower premiums.

Securities

In his testimony to the Senate Subcommittee on Commerce, Justice, State and the Judiciary on March 21, 2000, Chairman Arthur Levitt stated that Internet securities fraud is on the rise. He stated that there will be over 5.5 million online brokerage accounts by year end[11]. The SEC has seen a rapid rise in Internet fraud in this area, with most of it occurring in the past two years. One recent pyramid scheme raised more than $150 million from over 155,000 investors before it was shut down.

Securities fraud takes the form of stock manipulation, fraudulent offerings, and illegal touts conducted through newspapers, meetings, and cold calling, among others. These same scams have been conducted electronically, but are now joined by some newer, more sophisticated fraudulent activity. These include momentum-trading web sites, scalping recommendations, message boards posted by imposters, web sites for day trading recommendations, and misdirected messages. Investors are suffering large losses due to these cyber crimes.[12]

Telecommunications

The U.S. Secret Service estimates that telecommunication fraud losses exceed $1 billion annually.[13] Other estimates range from $3 billion to $12 billion.[14]

> Subscription, or identity fraud involves using false or stolen IDs or credit cards to gain free service and anonymity. It has tripled since 1997, says Rick Kemper, Cellular Telecommunications Industry Association's (CTIA) director of wireless technology and security, a trend he attributes to criminals favoring subscription fraud over cloning, plus increased industry competition to reach a broader and riskier market.[15]

.

The International Data Corporation (IDC: Framingham, MA) stated that, "Fraud remains endemic to the wireless industry, with estimated loses expected to reach a staggering $677 million by 2002…"[16] One of the key reasons is the dramatic increase of subscription fraud which IDC estimates will reach $473 million by 2002.[17]

Telemarketing fraud resulted in losses to victims of over $40 billion in 1998.[18] In 1996, the FBI estimated that there were over 14,000 telemarketing firms that were involved in fraudulent acts, the majority of which victimized the elderly. [19]

Many telemarketing firms have moved out of the United States to Toronto, Canada. They are able to attack American consumers from outside the country's borders. This poses a global challenge, as law enforcement agencies, in particular, need to work together.

Intellectual Property and Computer Crime

Intellectual property theft – in the form of trademark infringement, cyber squatters, typo squatters, trade-secret theft, and copyright infringement – has increased as Internet use and misuse has risen. It occurs across the seven industries detailed here, as well as most other businesses. "According to the American Society for Industrial Security, American businesses have been losing $250 billion a year from intellectual property theft since the mid-1990's."[20]

Identity Theft

Identity theft is not an industry specific crime. It can appear in any industry where personal information is used to gain credit or acquire customers. In years past, this type of crime was not prevalent, but the influx of technology has caused it to grow at a rapid pace and become a significant issue in the public eye, as its insidious nature poses real trauma to consumers. Statistics reflect its growth, with estimates of 500,000 to 700,000 victims of identity theft in 2000.[21] The growth of identity theft has reached epidemic proportions, and is quickly becoming the crime of the new millennium. The cost of investigating identity theft cases in 1997 was reported to be $745 million.[22] The cost to individuals, which the National Fraud Center conservatively estimates to be $50 billion a year, has prompted "Travelers Property Casualty Corp. to launch the first-ever insurance coverage for victims of identity theft. The coverage offers policyholders as much as $15,000 to cover expenses incurred in clearing their name."[23] According to the National Fraud Center, identity theft in e-commerce transactions is estimated at 11% of total transactions.

IMPACT OF TECHNOLOGY ON ECONOMIC CRIME

The United States economy, including the growing e-commerce aspect of it, is increasingly threatened by cyber economic crime. Multiple studies still show that fraud, security, and privacy continue to be the primary detriment to the growth of e-commerce. Most economic crimes have a cyber version today. These cyber crimes offer more opportunities to the criminals, with larger payoffs and fewer risks. Websites can be spoofed and hijacked. Payment systems can be compromised and electronic fund transfers to steal funds or launder money occur at lightning speeds. Serious electronic crimes and victimization of the public have caused consumer confidence to waiver. These issues have also lead to growing privacy concerns and demands. In turn, the reluctance of the American public to embrace e-Commerce fully is preventing this new form of business from

reaching its potential. We are quickly eroding the trust in our society that has been built up over the centuries.

GLOBAL IMPLICATIONS FOR ECONOMIC CRIME

The connectivity of the Internet has made the concept of borders and jurisdictions an incredible challenge in most situations and meaningless in others. Laws, policies, and procedures that were once the purview of sovereign states are now becoming the focus of the world community. Organized groups of criminals can easily commit economic crimes and avoid sanctions across what were once clearly defined jurisdictions, necessitating increased cooperation among the global criminal justice agencies.

Other threats include the loss of credibility with world partners, the transference of proceeds of economic crime to conventional crimes, such as drug trafficking and gun running, and threats to the national security by increased victimization from assaults based in foreign jurisdictions.

FUTURE NEEDS AND RECOMMENDATIONS

If the economic crime problem in the United States and the world is to be controlled the following areas must be addressed:

- Laws, regulations, and improved reporting systems. There are numerous bills pending in Congress that address criminal frauds committed on the Internet, identity theft, and issues involving Internet security and attacks upon web sites. This legislation should use language that will be easily adaptable to future technological changes to help deter economic crime. Further, legislative efforts will require broad based input in order to minimize the risk of onerous or restrictive legislation.

- Uniform and thorough reporting is necessary, as well; resources for prevention, investigation and prosecution will naturally follow as the enormity of the problem unfolds.

- Public-private partnerships must be fostered and enabled in order to prevent and combat economic and cyber crime. Strategies to develop and share tools and fraud databases need to be enacted.

- The increase in law enforcement budgets must be balanced between personnel, computer hardware and software to assist in the investigation and prosecution of economic and cyber crimes, and training to provide education on the problems and solutions. Economic and computer crime units in local and state law enforcement agencies should be trained in the detection, investigation and prosecution of economic and computer crime.

- There has been a sporadic increase in law enforcement personnel dedicated to investigating economic and computer crime. Both federal

and state governments have increased their budgets in these areas, and this trend will need to continue. There is a need for more support at the local level.

- Global interaction and cooperation. As economic and computer crime is a global problem, global interaction and cooperation must be fostered through multi-national organizations, treaties, safe harbors, alliances, and consistent laws.

- Balancing privacy interests. Personal or individual privacy concerns must be weighed against the needs for prevention, investigation and prosecution. Trust among law enforcement agencies, international governments, and private sector organizations must be fostered through discussions, a blend of regulation and industry self-regulation, and new technologies, so that the prevention and investigation process can go forward without impediment. Legal requirements for sharing information must be modified to foster cooperation. Safe harbors must be provided for organizations that are required to report and comply.

- A federal government body or sanctioned entity needs to have resources and must be focused, dedicated and empowered to facilitate, research and communicate methods of combating economic crime.

CONCLUSION

Preventing, detecting, investigating, and prosecuting economic crimes must become a priority, in an effort to lessen their impact on the economy and the public's confidence. However, both law enforcement and the private sector, as it stands now, is in danger of slipping further behind the highly sophisticated criminals. A greater understanding of how technology, competition, regulation, legislation and globalization is needed in order to successfully manage the delicate balance between economic progress and criminal opportunity. New resources, laws, support for existing organizations, e.g. The National Fraud Center, The National White Collar Crime Center, The Internet Fraud Council, The Economic Crime Investigation Institute, and public/private partnerships are necessary to control this growing problem in America and the world.

III. Growth of Economic Crime

ECONOMIC CRIME DEFINED

The lack of agreed upon definitions regarding economic crime and computer crime, has resulted in a paucity of data and information on the size and scope of the problem. There are no national mechanisms, such as the Uniform Crime Reports, for the reporting of economic crimes by law enforcement. Academics have not been able to agree on definitions and have for the most part continued to focus on white-collar crime. White-collar crimes require that the perpetrator be a person of status who has opportunity because of his position in an organization.[24] This definition, while seminal in the 1940's, is inaccurate today and impedes agreement on more contemporary definitions. Based on Sutherland's limited definition, all other crimes are viewed as newer versions of conventional crimes. Thus, the true nature of the amount of economic crime is buried in the statistics of more conventional crimes. For example, credit card fraud is typically classified as a larceny instead of access device fraud.

In 1995 the National Fraud Investigation Center undertook the task of creating a classification system that would be able to categorize and classify fraud information in a dynamic and hierarchical structure. The Fraud Identification Codes (FIC) were designed hierarchically to allow classification of each type of fraud in order of importance, and thus, provide the ability to add and modify types as it became necessary. Four levels of classification were developed, from the most general to the more specific: Class, Sub-class, Type and Sub-type. The following groups reviewed and recommended changes to the FIC: The Uniform Crime Reporting Division of the FBI, The National Incident Based Reporting System of the FBI, The White Collar Crime Division of the FBI, the American Bankers Association Check Fraud Unit, and the Secret Service. The FIC system currently has over 600 classified types of fraud including 11 classes, 75 sub-classes, over 350 types and over 175 sub-types. Without a framework and a single reporting center, economic crime statistics will continue to be fragmented estimates of the true extent of the level of the crimes. A system such as the FIC codes could provide the logical format for a national program to gather data on economic crimes.

In order to address the issue of economic crime in the United States, it is necessary to adopt a definition for the purpose of this white paper. The definition we will follow is:

> Economic Crime is defined as an illegal act (or a constantly evolving set of acts) generally committed by deception or misrepresentation (fraud) by someone (or a group) who has special professional or technical skills for the purposes of personal or organizational financial gain or to gain (or attempt to gain) an unfair advantage over another individual or entity.[25]

This definition provides for the inclusion of more contemporary crimes and methods in situations where the individual is not a person of status in an organization or even employed by the organization. It does not refer to these types of crimes as non-violent, as most definitions of white-collar crimes do. Increasingly, organized crime groups have used economic crime to fuel their enterprises, such as arms trafficking, drug smuggling, and terrorism, and have used violence to further their ends.

TYPES OF ECONOMIC CRIMES AND DEVELOPMENT OF STATUTORY LAW

There seems to be no limit to the types of economic crimes and the methods of committing them. However, certain crimes are unique to certain industries. For example, cloning applies to the wireless telecommunication industry and currency transaction reporting applies primarily to the banking and financial services industry. The discussion that follows relates to specific economic crimes in nine different areas and the laws enacted by Congress that proscribe the illegal conduct.

Mail and Wire Fraud: Generic Frauds and Swindles

The mail fraud statute (18 U.S.C. § 1341) was enacted in 1872. The law was designed specifically to enable special agents of the U.S. Mail to investigate frauds and swindles perpetrated through the use of the mail system and to seek federal prosecution for such offenses. Because it applies to "any scheme or artifice to defraud, or for obtaining money or property by false pretenses, representations or promises," the statute has been used to prosecute fraudulent insurance claims, fraudulent loan applications, securities frauds, and an unlimited variety of frauds and swindles. It frequently is applied to new types of fraudulent acts in those situations where Congress has not had the opportunity to enact a specific statute to deal with the crime. Because mail fraud has generic appeal, it applies to conventional economic crimes in the eight areas on which this report focuses.

The crime of mail fraud is committed by depositing or receiving matter with or from the Postal Service or a private interstate carrier (for example, FedEx or UPS) or causing matter to be delivered by the Postal Service or such carrier for the purpose of furthering the fraudulent scheme. There is no monetary threshold necessary for prosecution, although federal prosecutors informally may decline to handle minor cases.

The wire fraud statute (18 U.S.C. § 1343) is patterned after the mail fraud statute. It proscribes the use of interstate communications by wire, radio or television to perpetrate a scheme or artifice to defraud. The statute is generic in application and applies to a wide range of criminal activity across industries. Courts have not limited the reach of the statute to land line telephone communications; the statute has been applied to wireless communications using microwave

technology, in part. Because transactions over the Internet usually involve interstate communications by telephone wire or cable, the wire fraud statute will continue to serve as an effective law enforcement and prosecutorial tool to combat cyber crimes against all major industries.

Banking Industry: Financial Institution Crimes

Like mail and wire fraud, the bank fraud statute (18 U.S.C. § 1344) applies generically to any scheme to defraud a financial institution or any fraudulent act designed to obtain money or property from a financial institution. The statute currently defines a financial institution as any depositary institution insured by the FDIC, as well as credit unions and the Federal Reserve Bank. Unlike mail or wire fraud, which are limited to the medium of communication (either mail or wire), the bank fraud statute applies to any fraudulent scheme designed to obtain money or property from the financial institution, including check forging, check kiting, stolen checks, credit card fraud, fraudulent loan applications, student loan fraud, and embezzlement.

The financial statement statute (18 U.S.C. § 1014) applies to any fraudulent statement made to a financial institution for the purpose of obtaining money or property in the custody or control of the institution. The quintessential financial statement fraud is a false statement made in an application for a loan or to obtain credit from a financial institution.

The Continuing Financial Crimes Enterprise (CFCE) statute (18 U.S.C. § 225) was enacted in 1990 and is designed to impose criminal sanctions for large-scale frauds committed upon financial institutions, such as the massive frauds upon the savings and loan industry. A CFCE is a series of violations of numerous sections (215, 656, 657, 1005, 1006, 1007, 1014, 1032, or 1344) of title 18 of the U.S. Code, as well as the crimes of mail and wire fraud, if they affect a financial institution, committed by one who organizes, manages or supervises the enterprise, and receives $5 million in gross receipts from the enterprise over a 24-month period. It is limited to financial institutions as victims, but would include a series of credit card frauds, if those crimes were charged under 18 U.S.C. § 1341, 1343 or 1344.

The computer fraud statute (18 U.S.C. § 1030) currently prohibits accessing a “protected computer” without authority, or in excess of authority, to obtain information or to obtain something of value, hacking into a protected computer and transmitting a program, information, code, or command with the intent to damage the computer, or transmitting in interstate commerce any threat to cause damage to a protected computer in order to extort something of value. Because a “protected computer” includes a computer “exclusively for the use of a financial institution” or if not exclusively used, a computer “used by or for a financial institution * * * and the conduct constituting the offense affects that use by or for the financial institution” (18 U.S.C. § 1030 [e] [2]), the statute applies to specific

criminal conduct directed at bank computers or computerized data storage facilities.

The money laundering statutes (18 U.S.C. §§ 1956 and 1957) were enacted in 1986 as part of the Money Laundering Control Act. These sections apply to the conduct of the customer of a financial institution who deposits the proceeds of criminal activity with the bank and uses the bank to layer or launder those proceeds and to facilitate the transportation of the proceeds into or out of the country. Banks providing online services and electronic wire transfers are particularly susceptible to such conduct.

In 1970, Congress enacted the Bank Secrecy Act, also known as the Currency and Foreign Transaction Reporting Act, to curb the laundering of cash through banking institutions. That Act requires the filing of currency transaction reports (CTR's) for any deposit or withdrawal of cash exceeding $10,000. Subsequent amendments to the Act require the filing of reports for the transportation of currency or monetary instruments exceeding $10,000 into or out of the U.S., cash transactions exceeding $10,000 at casinos or as part of business transactions, and for suspicious activity transactions. The Treasury Department has promulgated several regulations providing the details of the reporting requirements, which apply to both electronic fund transfers and online banking transactions.

The Racketeering Influenced and Corrupt Organizations (RICO) statute (18 U.S.C. § 1962) has application to mail fraud, wire fraud, bank fraud, currency transaction reporting violations and money laundering because they are predicated acts constituting racketeering activity. RICO provides an effective law enforcement weapon against those who engage in a pattern of racketeering activity and victimize a financial institution, or those financial institutions that engage in a pattern of racketeering activity.

Credit Card Crimes

In addition to mail and wire fraud, Congress has enacted two laws that specifically address the traditional means of committing crimes involving a credit card. The credit card fraud statute (15 U.S.C. § 1644) prohibits the sale, use or transportation of a counterfeit, altered, stolen, lost or fraudulently obtained credit card in a transaction affecting or using interstate or foreign commerce, or furnishing money obtained through the use of a counterfeit, altered, stolen, lost or fraudulently obtained card, or the receipt or concealment of goods or tickets for interstate or foreign transportation obtained though the use of such a card. Federal courts disagree whether this crime can be committed without a plastic card. Because online transactions involve the use of the credit card number and not the card itself (although future technology might encompass the use of stored value, smart cards or some other form of encrypted card for Internet transactions), it is unclear whether section 1644 applies to online transactions.

The access device statute (18 U.S.C. § 1029), however, defines an "access device" to include a card (and thus, either credit, debit, stored value or "smart" cards) or an account number. This statute prohibits the production, use or trafficking in counterfeit credit cards or account numbers, the possession of 15 or more counterfeit cards or account numbers, producing, trafficking in or possessing equipment used to produce counterfeit cards, without authority from the card issuer, offering a card or selling information regarding applications to obtain cards, or attempts or conspiracies to commit any of the above acts regarding credit cards or account numbers.

Health Care Fraud

Prior to 1996, federal prosecutors employed generic crimes such as the false statements statute (18 U.S.C. § 1001), false claims statute (18 U.S.C. § 287), mail fraud statute (18 U.S.C. § 1341) or wire fraud statute (18 U.S.C. § 1343) to prosecute those charged with engaging in conduct encompassed by the term "health care fraud." In some instances, prosecutors were able to use laws created to address specific methods of committing health care fraud relating to the Medicare and Medicaid programs, such as the false claims statute (42 U.S.C. § 1320a-7b[a]), the anti-kickback statute (42 U.S.C. § 1320a-7b[b][1]), and the self-referral statute (42 U.S.C. § 1395nn). In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), which created five distinct health care fraud crimes. This enactment was significant in that it imposes criminal penalties for health care frauds perpetrated upon private health care benefit plans, as well as Medicare and Medicaid. "Health care fraud" under HIPAA is committed by executing or attempting to execute a scheme or artifice to defraud any health care benefit program or fraudulently obtaining the money or property of a health care benefit program (18 U.S.C. § 1347). HIPAA also proscribes the theft or embezzlement of funds, securities, premiums, property and other assets of a health care benefit program, concealment of a material fact or fraudulent statements in connection with the delivery or payment of health care benefits or services, and the obstruction of or interference with the communication of records relating to a violation of HIPAA to a criminal investigator (18 U.S.C. §§ 669, 1035, 1518). Additionally, a conspiracy to violate any of those offenses also is a crime (18 U.S.C. § 1345).

Federal financial statement fraud (18 U.S.C. § 1001) and false claims fraud (18 U.S.C. § 287) have limited application to the health care industry because the victim in those statutes is the government. The enactment of HIPAA significantly enhances the prosecutorial arsenal available to combat health care fraud committed by traditional means because the victim of those crimes are health care benefit programs, which include private health insurance plans. The Act, however, does not address a myriad of other cyber crimes that are health care related, for example, pharmaceutical fraud, web sites that fraudulently purport to

provide medical advice, and phony web sites. The only statutory tool currently available to prosecute such conduct effectively is the wire fraud statute.

Insurance Fraud

Most fraudulent conduct impacting upon the insurance industry constitutes application fraud or claims fraud. These frauds may be committed by the insured, an agent or employee of the company, a third party, or as is more often the case, a conspiracy between two or more of those groups. Historically, insurance fraud has been the subject of state regulation. Nevertheless, federal jurisdiction and laws may be invoked where the fraudulent activity constitutes a mail or wire fraud, which is frequently the case. Applications for insurance are commonly sent through the mail or processed online over the Internet. Proofs of loss, bills, invoices and receipts submitted in support of an insurance claim typically are transmitted to the insurer by mail or by fax transmission. Further, a continuing pattern of such activity may constitute a RICO crime.

Federal law (18 U.S.C. § 1033) also regulates the conduct of persons or entities engaged in the business of insurance. It imposes criminal sanctions for (a) the embezzlement or misappropriation of premiums, money or other property of insurance companies, (b) the making of false statements or reports to an insurance regulatory agency or official involving the overvaluing of land, property or security for the purpose of influencing action by that agency, (c) making false entries in any book, report or statement of the insurance company to deceive the company or an insurance agency or official regarding the financial solvency of the business, (d) engaging in the insurance business by any person convicted of a felony involving dishonesty or a breach of trust, and (e) threatening, influencing or obstructing the administration of law in any pending proceeding before an insurance regulatory agency or official. There is no published decision to date regarding prosecutions under this section. Section 1034 authorizes the U.S. Attorney General to seek civil penalties or injunctions for violations of section 1033.

Securities Fraud

Congress created numerous securities fraud crimes by enactment of the Securities and Exchange Act of 1934. The major anti-fraud statute is section 10(b) of the Act, which is codified at 15 U.S.C. § 78j (b). That section and Rule 10b-5 (7 C.F.R. § 240.10b-5), which was promulgated by the Securities Exchange Commission, prohibit the use of any instrumentality of interstate commerce or stock exchange or mail for the commission of a fraudulent act, scheme or artifice to defraud, or the making of a false statement in connection with the purchase or sale of a security. Although that statute and rule have served as an effective prosecutorial weapon in combating securities fraud and insider trading, the statute was not drawn with the Internet and e-trading in mind.

Telecommunication Fraud

Fraud impacts all sectors of the communications industry—telephone, wireless, and cable. The types of fraud are numerous: toll fraud, including "clip-on" and "shoulder surfing" methods, call-sell operations established by organized crime groups who engage "phreaks" to hack into phone line, subscription fraud, which frequently also involves identity theft, PBX fraud, which also involves call-sell operations, calling card fraud, remote call forwarding, and computer terrorism/sabotage. Because these frauds frequently encompass interstate wire communications, the wire fraud statute is an effective legal weapon to combat telecommunication fraud.

The principal fraudulent activities impacting upon the wireless communication industry are subscription fraud and cloning. Subscription fraud occurs when an individual applies for and obtains a wireless telephone account. Because a fraudulent application customarily involves the use of a counterfeit or stolen credit card or account number, or a stolen means of identification, the credit card fraud, access device fraud, and identity fraud statutes are available for the prosecution of such behavior. Most wireless service providers currently encourage customers to apply by accessing their web site. The wire fraud statute serves as an additional prosecutorial weapon to combat online subscription fraud.

Cloning entails the theft of an electronic serial number (ESN) and mobile identification number (MIN) assigned to a legitimate wireless phone, and the installation of those numbers on a stolen phone. Once accomplished, the cloned stolen phone behaves like the phone owned by the legitimate customer, and the monthly bill for charges are sent to the legitimate customer. The access device statute (18 U.S.C. § 1029) specifically proscribes the theft of ESNs and MINs, the production or use of a cloned phone, and the possession, use, production or trafficking in scanning receivers or hardware or software utilized to clone phones for the purpose of obtaining unauthorized wireless services. Although cloning a phone and the use of a cloned phone historically has not involved the Internet, technology is now in place to enable wireless access to the Internet. The access device statute should continue to be an effective legal weapon to combat the use of cloned phones for Internet access. Additionally, the computer fraud statute may also apply to such conduct.

Congress initially sought to regulate abuses committed by the telemarketing industry by enactment of the Telephone Consumer Protection Act of 1991 (47 U.S.C. § 227). That Act provides for statutory damages for each violation, but does not impose criminal sanctions. In 1994, Congress enacted the Senior Citizens Against Marketing Scams (SCAMS) Act. The SCAMS Act (18 U.S.C. §§ 2325-2327) imposes criminal penalties for telemarketing frauds involving wire communications, including conspiracies to commit such crimes, and enhanced sentences where senior citizens are victimized. Because Internet scams

encompass the use of wire communications in part, the wire fraud statute (18 U.S.C. § 1343) will remain an effective legal weapon for the prosecution of scammers.

Intellectual Property and Computer Crime

The computer fraud statute (18 U.S.C. § 1030) seeks to address conduct involving the use of computers to perpetrate the crime and computers as the victims of crime. The statute imposes criminal penalties for:

(1) Accessing a computer without authorization to obtain classified federal information to be used for the benefit of a foreign nation.
(2) Accessing a computer without authorization to obtain the financial record of a financial institution, issuer of a credit card, consumer reporting agency or federal agency.
(3) Accessing a government computer without authorization and affecting the government's use of the computer.
(4) Accessing a protected computer (a "protected computer" is a computer either used in interstate or foreign commerce or exclusively for the use of a financial institution or the U.S. government) without authorization and with the intent to defraud and obtaining anything of value through that fraudulent act.
(5) Transmitting a program, information, code or command and intentionally causing damage to a protected computer.
(6) Accessing a protected computer and causing damage.
(7) Trafficking in any password that can be used to access a computer if the trafficking affects interstate or foreign commerce, or "such computer is used by or for the Government of the United States."[26]
(8) Transmitting any threat to cause damage to a protected computer in order to extort money or other thing of value.

To the extent that credit card account numbers constitute computer data on various e-commerce web sites, accessing the computers or peripheral equipment for the purposes of unlawfully obtaining and trafficking in stolen account numbers may also constitute computer fraud. A recent example of such conduct is the hacker identified as Maxim who attempted to extort $100,000 from CD Universe and, when the threat failed, posted credit card account numbers that he had obtained from CD Universe's web site on another web site.

Because the use of a modem involves a wire communication, the wire fraud statute (18 U.S.C. § 1343) applies to the use of a computer to commit crimes, including credit card transactions, online banking, online insurance fraud, etc.

Prior to 1996, the principal federal weapon designed to combat the theft of trade secrets was the Trade Secrets Act (18 U.S.C. § 1905). That statute prohibits the unauthorized disclosure of confidential information by government employees.

Prosecutions for trade secret theft that victimized the private sector were based on the National Stolen Property Act, which was not particularly effective because it did not encompass intangibles (soft property) within its protective embrace, or the mail or wire fraud statute. The Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839) attempted to cure previous deficiencies by imposing criminal penalties for economic espionage by or for foreign government and for the theft of trade secrets from public and private sector sources. Moreover, the 1996 statute defines the theft of trade secrets to include a misappropriation committed by any means, as well as the receipt of trade secrets.

The Trademark Counterfeiting Act of 1984 (18 U.S.C. § 2320) imposes criminal penalties for the intentional trafficking in counterfeit goods and services, i.e., those goods and services that bear a stolen trademark.

Congress first imposed criminal sanctions for copyright infringements in 1897. Since that time, the statute (currently 18 U.S.C. § 2319) has been amended on numerous occasions as Congress attempted to provide more protection to the copyright holder. Notably in 1992, the Copyright Felony Act added protection against large-scale computer software privacy, and in 1997 Congress enacted the No Electronic Theft Act, which removed the requirement that the perpetrator derive a financial gain from the infringement.

Identity Theft

The federal identity fraud statute (18 U.S.C. § 1028) prohibits the unlawful production, possession, transfer or use of a "means of identification" of another person to commit or abet any federal crime or state felony crime or to defraud the federal government. The statute defines a "means of identification" as any name or number used to identify an individual, including an access device. Because access devices include a credit card account number, the crime of identity fraud encompasses the use of another person's credit card account number, as opposed to use of the plastic card itself. The statute also includes other devices as "means of identification," including a passport, birth certificate, driver's license, social security number, taxpayer identification number, unique electronic identification number (e.g., user ID or password), and unique biometric data, such as a fingerprint, voice print, retina or iris image.

By 1999, twenty states had enacted identity theft statutes.[27] Many other states prosecute identity theft under criminal impersonation statutes. The success of identity theft prosecutions under those impersonation statutes depends upon the language of each statute.

IV. IMPACT OF TECHNOLOGY ON ECONOMIC CRIME

The growth of the information age and the globalization of Internet communication and commerce have impacted significantly upon the manner in which economic crimes are committed, the frequency with which those crimes are committed, and the difficulty in apprehending the perpetrators. A recent survey conducted by the Gartner Group of 160 retail companies selling products over the Internet reveals that the amount of credit card fraud is twelve times higher online than in the physical retail world.[28] There is no reason to believe that this figure is unique to the credit card industry. Another recent study indicates that the number of search warrants issued by the federal government for online data has increased 800% over the past few years.[29] Technology has contributed to that increase in four major respects—anonymity, security (or insecurity), privacy (or the lack of it) and globalization. Additionally, technology has provided the medium or opportunity for the commission of traditional crimes. Criminals continue to make false statements in credit applications submitted over the Internet, bank employees continue to embezzle funds by wire transfer or account takeover, and swindlers continue to misrepresent products at auction sites over the Internet. However, it is the widespread use of technology and the Internet for business transactions and communications, and the confluence of anonymity, security, privacy and globalization that have exposed the public and private sectors to an alarming new array of cyber attacks. In addition to their inability to prevent such attacks, both government and the private sector lack effective enforcement tools and remedies to bring the perpetrators to justice.

Technology and the Internet have contributed to the growth of economic crime in each of the identified industries in similar ways. Anonymity enables the criminal to submit fraudulent online applications for bank loans, credit card accounts, insurance coverage, brokerage accounts, and health care coverage or to construct a counterfeit web site in order to establish an inflated value for publicly traded stock in order to sell the stock at a falsely inflated price ("pump and dump" schemes). Anonymity also enables employees to pilfer corporate assets. For example, bank employees can embezzle money through electronic fund transfers and employees of credit card issuers can capture account numbers and sell them to outsiders, electronically transferring the account numbers to the co-conspirators. Further, anonymity provides enhanced opportunities for two types of perpetrators—the organized crime mobster and the teenage hacker.

Security, or the lack of it, enables criminal hackers to disrupt e-commerce in several ways. They can engage in denial of service attacks, compromise payment systems in online banking, penetrate web sites and extract credit card account numbers for resale or as ransom for the extortion of cash from the card issuer, or hijack a web site for the purpose of stealing the identity of the e-commerce merchant, directing the proceeds of sales to the hijacker.

Privacy protections enable thieves to take advantage of the benefits of anonymity, while hampering the efforts of law enforcement and private sector fraud investigators to track the thieves. Lastly, the Internet enables communication and commerce to occur beyond or without borders, presenting significant problems in the prevention, investigation and enforcement of those crimes.

Banking

There is no pending legislation that specifically addresses frauds in connection with online banking. The Internet provides fertile ground for those intending to defraud financial institutions. Because the online customer is anonymous, the risk of fraud is greater. Projected increases in the volume of online transactions and repeal of the Glass-Steagall Act, which has expanded the types of institutions that may provide banking services, could increase the exposure to cyber attack. Congressional focus is currently on cyber laundering, specifically the electronic transfer of funds into U.S. banks from sources outside the country and subsequent transfers by those banks to cyber laundering havens. On the regulatory side, the Federal Trade Commission and other agencies have proposed regulations dealing with the privacy of financial data, the circumstances when disclosure may be made, and the conditions precedent to such disclosures. Those regulations, which are scheduled to take effect on November 13, 2000, require financial institutions to provide privacy notices to consumers, limit the disclosure of nonpublic personal information to nonaffiliated third parties, and allow consumers to opt-out of certain restrictions.

The Electronic Signature in Global and National Commerce Act, which became law on July 1, 2000, is a major effort to facilitate the consummation of contracts, including agreements with banking and financial institutions, electronically. While the Act facilitates e-Commerce, it provides yet another opportunity for the theft of a significant aspect of one's identity—the signature. The Act contains no provision imposing criminal sanctions for the theft or piracy of one's signature. The access device statute (18 U.S.C. § 1029) should be amended to include electronic and digital signatures as a "means of identification. Additional legislation is essential to reduce the risks presented by anonymity and database insecurity, including prescribed authentication procedures and encryption protections.

Credit Card

The use of credit cards for online retail purchases, as well as for online gambling and to gain access to pornography and child pornography sites, is expected to increase exponentially. Online transactions are not conducted face-to-face; therefore, the merchant cannot identify the customer in the traditional manner. The increased volume of online transactions and the absence of face-to-face

interaction provide greater opportunity for fraud, including identity theft for the purpose of conducting an online transaction. While substantive laws provide ample redress for the criminal use of credit cards (and debit cards) in cyberspace, the implementation of new technologies for credit purchases, such as smart cards and electronic wallets, may raise issues regarding the applicability of existing criminal statutes. Those statutes (specifically 15 U.S.C. § 1644 and 18 U.S.C. § 1029) should be amended to prohibit the theft or fraudulent sale, distribution or possession of a counterfeit, stolen or fictitious account number regardless of whether that account number is used in connection with a plastic card, electronic wallet or other form of digital storage. The amendment should also state that the crime applies to the theft by computer of account numbers or information that could be used to identify an account number.

There is currently no pending legislation that would regulate the use of credit cards for online transactions. However, S. 699, the Telemarketing Fraud and Seniors Protection Act, would amend the wire fraud statute (18 U.S.C. § 1343) to include schemes or artifices to defraud, perpetrated via Internet communications. Because credit card fraud can be prosecuted under this statute, the proposed legislation would enhance significantly the enforcement arsenal for credit card fraud. Further, the proposed Identity Theft Protection Act of 2000 (S. 2328) would strengthen protection against fraudulent practices committed with stolen credit cards. That Act requires the card issuer to confirm any reported change of address and notify the cardholder of any request for additional cards. It also requires credit-reporting agencies to inform the card issuer if the address on the application for a credit card is different than the address shown in the consumer's records. Section 4 of the Act would also add a requirement that, upon the request of the consumer, a consumer reporting agency must include a fraud alert in the consumer's file and notify each person seeking credit information of the existence of that alert. That Act would provide significant protection from the technological identity theft.

Health Care

Currently, there is no pending legislation designed to address health care frauds committed in cyberspace. Future legislative attention should focus on the attributes of the Internet and e-commerce that promote fraudulent activity in the provision of health care products and services.

Insurance

There currently are no pending federal laws or regulations that address insurance fraud committed in cyberspace. Historically, regulation of the insurance business has been the province of the states. The 1999 Gramm-Leach-Bliley Act, which repealed the Glass-Steagall Act, enabled financial institutions to provide a variety of services, including insurance. The federal government should establish broad legislation designed to regulate and secure

the online sale of insurance products. Arguably, the only effective weapon at the disposal of federal prosecutors is the wire fraud statute. Additional legislation that requires secure connections and seeks to prevent fraudulent activity regarding online insurance applications and claims should be a priority. Moreover, because the Internet is an instrument of interstate commerce, Congress should rethink that portion of the Gramm-Leach-Bliley Act which leaves the regulation of issues such as the use of nonpublic information by insurance companies to the state regulators. Federal involvement in this area would provide uniform regulation and would not subject financial institutions that provide banking, securities and insurance products to a different regulatory scheme for the offering of insurance products.

Securities

The Internet is an instrument of interstate commerce. Thus, section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 provide criminal sanctions for fraudulent [30]acts committed in cyberspace involving the purchase or sale of securities. Also, the mail fraud and wire fraud statutes provide an additional weapon for the prosecution of frauds and swindles involving securities. Again, substantive criminal laws provide ample sanction for fraudulent conduct impacting upon the securities industry.

The Securities Exchange Commission is, however, faced with the difficult task of detecting and investigating securities frauds committed in the online venue. It has created a new enforcement unit to deal specifically with online trading and frauds committed with respect to securities, but legislation is required to assist investigators in the detection and investigation of such frauds. The Online Investor Protection Act of 1999, S. 1015, would be a start in that direction.

Telecommunications

As noted above, S. 699, The Telemarketing Fraud and Senior Protection Act would amend the wire fraud statute (18 U.S.C. § 1343) to prohibit fraudulent telemarketing practices over the Internet. That statute should be further amended to prohibit fraudulent conduct over the Internet transacted in part through a wireless connection.

Intellectual Property and Computer Crime

Although existing criminal laws will continue to provide effective weapons to combat cyber crimes committed upon the traditional service industries that offer their services and products through e-commerce, Congress and the global community must move swiftly to provide an effective array of substantive laws designed specifically for Internet transactions. That array should include laws and treaties to provide law enforcement and the private sector with the tools essential for the detection and investigation of cyber crime. Some Congressional

attention has focused on peripheral issues such as privacy and encryption, and there are signs that Congress is beginning to address Internet-specific issues. Five pending Congressional bills suggest that Congress is aware that law enforcement must be equipped with adequate resources and remedies to combat cyber crime.

.

A High Tech Crime Bill (S. 2092) was introduced on February 24, 2000 by senators Charles Schumer and John Kyl. This bill proposes amendments to the computer fraud statute (18 U.S.C. § 1030) that would include fraudulent acts committed upon "protected computers" in the United States, by persons in foreign countries and would include damage done to computers and computer systems irrespective of property damage losses. That amendment would encompass damage caused by, for example, denial of service attacks. The proposed bill also would amend 18 U.S.C. § 3123 (c), enabling law enforcement to employ trap and trace devices to assist in the investigation of computer attacks.

The Internet Security Act of 2000 (S. 2430), introduced in April 2000 by Senator Leahy, would expand the jurisdictional scope of the computer fraud statute to include international hacking. It would amend section 3123 to enable law enforcement to employ trap and trace devices, impose encryption standards, and authorize the prosecution of juvenile hackers. It would also appropriate $25 million for each of the next four fiscal years for law enforcement training programs in computer fraud investigations. Both bills seek to react to recent attacks upon e-Commerce sites, including the denial of service attacks.

The Internet Integrity and Critical Infrastructure Protection Act of 2000 (S. 2448), introduced on April 13, 2000 by Senator Hatch, co-sponsored by Senator Schumer, would impose criminal penalties for cyber hacking committed by persons under 18 years old, create a National Cyber Crime Technical Support Center to serve as a resource center for federal, state and local law enforcement and assist them in the investigation of computer-related crimes, and provide the implementation of computer crime mutual assistance agreements in order to enable reciprocal assistance for foreign authorities.

Also on April 13, 2000, Senator Hutchinson introduced S. 2451 that would increase the criminal penalties for computer fraud committed in violation of 18 U.S.C. § 1030 and establish a National Commission on Cybersecurity to study incidents of computer crimes and the need for enhanced methods of combating such crimes.

Finally, on May 9, 2000, Congressman Boehlert introduced the Law Enforcement Science and Technology Act of 2000 (H.R. 4403), co-sponsored by Congressman Stupak. This bill would establish an Office of Science and Technology in the Office of Justice Programs of the Department of Justice. The mission of that Office would be “(1) to serve as the national focal point for work

on law enforcement technology; and (2) to carry out programs to improve the safety and effectiveness of, and access to, technology to assist Federal, State and local law enforcement agencies."[31] The bill would direct the appropriation of $40 million for regional National Law Enforcement and Corrections Technology Centers, $60 million for research and development of forensic technologies and methods to improve crime laboratories, and $20 million for the testing and evaluation of technologies.

Additional governmental attention must be focused on extradition and mutual assistance treaties that will enable the United States to prosecute cyber crimes committed by international terrorists and hackers.

V. Victims of Economic Crime

Consumers

Very few studies on fraud victimization have been conducted. Two that studied telemarketing are Harris and Associates[32] and a study by the American Association of Retired Persons.[33] The most comprehensive study to date is the National White Collar Crime Center's National Public Survey on White Collar Crime.[34] The study's goal was, "to present a picture of what the average American thinks about white collar crime."[35] Its survey of 1,169 households throughout the United States found that:

- Over 1 out of 3 households had been victimized by white collar crime in the last year.
- Widely held opinions concerning the profile of typical white collar crime victims are divorced from the actual profile of victims found by recent research on victimization
- There is a disparity between how Americans believe they will react if victimized and how they do react when they are actually victimized.
- Less than 1 in 10 victimizations were ever reported to law enforcement or consumer protection agencies
- The public has a deep concern with increasing the apprehension and sanctioning of white collar criminals.[36]

Consumer victimization usually results in three types of losses: privacy, good credit status, and funds or assets. Consumers are concerned that personal information disclosed to companies with which they do business may be compromised. Such compromises include unauthorized access and/or by the company's employees, lack of security to protect the information, providing the information to third parties, and the maintenance of accurate information. Any one of these breaches could result in the consumer's personal information falling into criminal hands, which could easily result in identity theft. Other consequences range from damage to an individual's credit rating to the loss of funds and/or assets.

Industry

The victimization of industry falls into four categories:

- Profit losses
- Damage to reputation
- Loss of continuity of business
- Loss of intellectual property

According to The Credit Risk Management Report, "The average organization loses more than $9 a day per employee to fraud and abuse. The average organization loses about 6 percent of its total annual revenue to fraud and abuse committed by its own employees. Fraud and abuse costs US organizations more than $400 billion annually."[37] Early on, many corporations were able to take the position that fraud was a cost of doing business, and could make it up by passing the cost of fraud to the consumer through increased prices. In more competitive markets this is not possible. In those cases when the bottom line is hit hard by fraud, executives are less reluctant to commit funds to fraud management and computer security. While big business can sustain a major loss to fraud, many small businesses have suffered severely and in some cases have gone out of business as a result of their fraud losses. This often occurs because these small organizations cannot afford sophisticated hardware and software to prevent and detect fraud.

Because corporations are afraid that reporting fraud may damage their reputation, they are reluctant to do so. They fear legal retaliation if they share or disclose too much, and are afraid that their consumers and stockholders will lose confidence in them. The actual amount of corporate victimization is not known, because of the unwillingness of corporations to report or admit that fraud has affected them.

Many e-Businesses are concerned about the continuity of their business. That is, they do not want their services to customers to be disrupted. Although security remains a significant concern for business, consumers are paramount in e-Commerce; they want to shop quickly with no hassles. Recent distributed denial of service attacks on web sites such as e-bay and Amazon.com point to the vulnerabilities of e-Commerce. The lack of security and the intrusion of criminals (fraudulent element) both impede the growth of e-Commerce.

Intellectual property theft – in the form of trademark infringement, cyber squatters, typo squatters, trade-secret theft, and copyright infringement – has increased as Internet use and misuse has risen. It occurs across the seven industries detailed here, as well as most other businesses. "According to the American Society for Industrial Security, American businesses have been losing $250 billion a year from intellectual property theft since the mid-1990's."[38]

Government

Government suffers from several forms of victimization, much like corporations do, including theft of intellectual property, theft of assets, and loss of reputation. Several cases have been in the news where United States secrets have been compromised or potentially compromised. These events have tarnished the reputation of several government agencies by pointing out the lack of, or loose, security procedures.

Numerous federal governmental web sites have been defaced by hackers, including the CIA, FBI, and the United States Department of Justice. Several reports of intrusions have occurred with government computers. In many of these cases, systems have been penetrated, but no classified information was accessed.

Fraud, waste, abuse, and mismanagement are generally reported together. While it is hard to get a handle on their size and scope, the Senate Governmental Affairs Committee, chaired by Senator Fred Thompson (R-Tennessee) reported on January 26, 2000, that "In 1998 alone, $35 billion in taxpayer dollars was lost due to government waste, fraud, abuse, and mismanagement."[39]

VI. Waging the War on Economic Crime

Law Enforcement

On the federal level, numerous regulatory and law enforcement agencies are authorized to combat specific economic crimes, including the Federal Bureau of Investigation (FBI), United States Secret Service (USSS), the United States Postal Inspection Service, Securities and Exchange Commission (SEC), and United States Customs. Each of these agencies has jurisdiction over the following economic crimes/fraud.

- FBI – health care, financial institution, intellectual property, telemarketing, securities/commodities, bankruptcy, insurance, computer, and Internet
- Secret Service – credit card, cellular, and computer
- Postal Inspector – mail and consumer
- Securities and Exchange Commission -- insider and online trading, stock manipulation, and fraudulent stock offerings
- United States Customs – money laundering, cyber crimes, including child pornography and the importing of dangerous substances

On the international level, Interpol recently announced its intention to become active in the investigation of international computer crimes. Interpol announced on June 30, 2000 that it is establishing an international intelligence network to inform the public and private sectors of impending cyber attacks and potential targets for malicious hacks. The intelligence information will be relayed to Interpol by Atomic Tangerine, a venture consulting firm, using technology (Net Radar) developed by SRI International, the parent company of Atomic Tangerine.[40]

Local law enforcement capabilities for combating economic crime vary depending on the size and location of the department, and the allocation of resources. Some larger municipalities and state law enforcement agencies have formed economic and computer crime units. As resources, training, and awareness of the intensity of the problem increase, it is likely that more of these units will be formed.

National Fraud Center

The National Fraud Center (NFC) is an internationally recognized leader in global customized fraud and risk management solutions. Formed in 1982, its original mission was to combat insurance fraud, which, at that time, was becoming a societal concern. Since then the NFC has earned a reputation for combining expert knowledge and technology to produce solutions to fraud problems for vertical industries and the government. "Technological solutions developed with NFC's expertise have saved clients tens of millions of dollars."[41] The NFC has an in-depth understanding of how economic crime affects businesses,

consumers, and government agencies, as its researchers collect and analyze fraud data continuously.

Economic Crime Investigation Institute

The Economic Crime Investigation Institute (ECII) was formed in 1988 by Dr. Gary R. Gordon, then Director of the Economic Crime Investigation program at Utica College of Syracuse University, and Mr. John Martin, Esq., then Chief of Internal Security for the United States Department of Justice. Part of the Institute's mission is to support education and research in the areas of economic crime and computer security, by advising Utica College faculty on formal academic programs for pre-professional students and professionals in the field of economic crime investigation. Its other goal is to develop the ECII into the premier educationally focused institute, providing a national forum that brings together all interested parties to develop solutions to economic crime problems faced by society. The ECII strives to provide a forum for individuals in government, corporate America, and higher education to discuss current economic crime issues and to promote the dissemination of information on economic crime and its investigations. The Economic Crime Investigation Institute's annual conferences are its primary way of accomplishing this. [42]

National White Collar Crime Center

A non-profit organization that receives federal grant funding from the Bureau of Justice Assistance, Department of Justice, the National White Collar Crime Center (NW3C) "provides a nationwide support network for enforcement agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime."[43] Founded in 1980, the Center's focus is to support state and local agencies, using their needs as a guide for the projects and endeavors the NW3C undertakes.

In addition to its state-of-the-art financial and computer crime training course development and delivery, new projects include the development of the National Fraud Complaint Management Center (NFCMC) to leverage technology in the management of economic crime complaints and to bring added value to the prevention, investigation, and prosecution efforts surrounding complaints. A significant part of this project is the establishment of the Internet Fraud Complaint Center (IFCC) in partnership with the Federal Bureau of Investigation. The IFCC represents a unique approach to the growing problem of fraud on the Internet.

The NW3C has also been selected to serve as the Operations Center for the National Cybercrime Training Partnership (NCTP), an initiative of the United States Attorney General, headed by the Computer Crimes and Intellectual Property Section of the Justice Department.

The National Coalition for the Prevention of Economic Crime

A non-profit organization established in 1996, the National Coalition for the Prevention of Economic Crime (NCPEC) provides support services to businesses in their fight against economic crime. Its mission is to reduce incidents of economic crime through cooperative, information-sharing efforts.

Current training programs include instruction on fraud management, operational and strategic fraud management techniques, financial investigations practical skills, basic data recovery and analysis and instruction on how to use the Internet as an investigative tool.

Hosted in partnership with the NW3C, the NCPEC has established an annual national conference entitled the Economic Crime Summit which brings together academics, government, private corporations, victims' interest groups, prevention specialists, and others to examine methodologies and share ideas to address economic crime on all levels.

Internet Fraud Council

The Internet Fraud Council, a division of the National Coalition for the Prevention of Economic Crime, is composed of organizations from around the world that are interested in the prevention, investigation, and prosecution of Internet fraud. The Internet Fraud Council's mission is to provide research, education, best practices, and tools for the prevention of economic crime committed using the Internet.[44].

Internet Fraud Complaint Center

The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IFCC's mission is to address fraud committed over the Internet.

For victims of Internet fraud, IFCC provides a convenient and easy way to alert authorities of a suspected criminal or civil violation. For law enforcement and regulatory agencies, IFCC offers a central repository for complaints related to Internet fraud. The data from this source can then be analyzed to identify and quantify fraud patterns, as well as statistics on the current fraud trends.

The IFCC's ultimate goal is to reduce Internet fraud victimization. As stated on its web site, "Long term benefits of this program will be substantial. Not only will its efforts reduce the amount of economic loss by Internet fraud throughout the United States, it will enable state and local law enforcement professionals to develop and successfully prosecute criminal Internet fraud cases. IFCC will also

serve as the catalyst that allows law enforcement and regulatory authorities to network and share fraud data."[45]

Independent Corporations and Private Sector Industry Coalitions

As a result of limited law enforcement resources, corporations on their own or in cooperation with industry coalitions, such as BITS, the technology group for the Financial Services Roundtable, have had to initiate strategic economic crime management plans and investigative groups. There is a growing level of frustration among these corporations, because the monetary thresholds for law enforcement even to investigate a case, let alone prosecute, can be very high, depending on the jurisdiction. Coupled with this, is increased legislation requiring corporations to institute anti-fraud programs and compliance departments. While the protection of corporate assets and their consumers should be their responsibility, there are several consequences to this arrangement. Many economic crimes go unreported, fewer prosecutions of these offenses occur, and perpetrators tend to be fired rather than prosecuted, leaving them free to move on to another organization and continue their victimization.

VII. Future Needs and Challenges

Law Enforcement Training

Specialized training in the areas of economic and computer crime, and how they affect specific industries, as well as computer forensics, needs to continue to increase for law enforcement personnel. Without an understanding of how specific industries function, it is difficult to investigate or prosecute economic crimes. New career paths within law enforcement organizations could be established before promotions and reassignments drain agencies of their limited skilled personnel in technically sophisticated areas. Often, individuals develop expertise and then are promoted or reassigned, making it necessary to train new people from ground zero. Unless the individuals who have expertise, experience, and contacts in industry are given an incentive to stay in their units, this cycle will continue and the investigation and prosecution of economic crime will not increase or improve.

Laws, Regulations and Reporting Systems

In the United States, government (federal, state and local), with limited exceptions, has allowed self-regulation of the Internet. Government regulation has, for the most part, focused on cyber crimes that are not economic crimes, such as child pornography and cyber stalking. Fortunately, that attitude appears to be changing. There are numerous bills pending in Congress that address criminal frauds committed on the Internet, identity theft, and issues involving Internet security and attacks upon web sites. This legislation should use language that will be easily adaptable to future technological changes to help deter future economic crimes.

However, there are other gaps in legislation. There are many regulations that require businesses to protect themselves by working to prevent fraud (i.e. know your customer). However, the government sends conflicting signals when it will not assist in prevention efforts by cleaning up regulations and enacting new supporting laws, as well as providing prosecutorial support. Current government regulations covering certain industries prohibit companies from sharing information with each other. This eliminates the possibility of an instrument, such as a central database of fraud, which companies could use in their procedures for preventing and detecting fraud. It is important that legislation addressing this be written and passed. Other legislation is also necessary, such as laws that keep pace with the changing nature of credit card payment and online payment systems.

Public-Private Partnerships

No one group will be able to solve the complex problem posed by economic crime. Coalitions of private and public groups need to work together to combat economic and cyber crime. The onset of groups such as those mentioned above (e.g. ECII, NW3C, BITS) is encouraging. As more of these alliances develop, there will be more resources available to reverse the trend of economic crime. College and universities need to revamp their existing programs, e.g. criminal justice, accounting, computer science, or create new ones to meet the changing needs of society in this area. At this time there are only two undergraduate programs and one graduate program addressing these issues – the Economic Crime Investigations Programs at Utica College (Utica, NY) and Hilbert College (Hamburg, NY) and the Economic Crime Management Master's Program at Utica College. These programs are supported by advisory boards consisting of individuals at the top of their fields from the credit card, banking, insurance, and telecommunications industries, as well as representatives from government agencies, such as the U.S. Secret Service and the FBI. Further Congress, through the Identity Theft Assumption and Deterrence Act requires the FTC and industry to work together. Presidential Directive 63 (PDD 63) required industry and government to work together in combating Internet/e-commerce fraud.

Balancing Privacy Interests

The growth of e-commerce and the creation of new law enforcement techniques to combat cyber crime raise critical issues concerning consumer, business and governmental privacy. The protection of individual privacy, while considered almost sacred, in the world of economic and cyber crime can actually work to the criminal's advantage. The new FBI tool, Carnivore, is an attempt to gather intelligence information, without compromising privacy. According to the FBI's web site,

> In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet service providers (ISP) lack the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others, the FBI designed a diagnostic tool, called Carnivore.
>
> The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are subject of the lawful order while ignoring those communications which they are not authorized to intercept.

> This is a matter of employing new technology to lawfully obtain important information, while providing enhanced privacy protection.[46]

Carnivore provides law enforcement with the ability to keep pace with the technical advances in communication. However, this tool raises "Big Brother" concerns for the public. The controversy that Carnivore has evoked in its infancy points to the issue of trust that government, industry, and society as a whole need to resolve.

BITS, Financial Services Roundtable adopted privacy principles in late 1997 that are guidelines for banking industry self-regulation concerning privacy. Industry, in general, sees self-regulation as preferable to government rule. The BITS policy includes guidelines in each of these areas.

1. Recognition Of A Customer's Expectation Of Privacy
2. Use, Collection, And Retention Of Customer Information
3. Maintenance Of Accurate Information
4. Limiting Employee Access To Information
5. Protection Of Information Via Established Security Procedures
6. Restrictions On The Disclosure Of Account Information
7. Maintaining Customer Privacy In Business Relationships With Third Parties
8. Disclosure Of Privacy Principles To Customers

Several other industry organizations are developing similar guidelines. Their aim is to have self-regulation rather than government intervention. By informing customers of privacy policies, industry is attempting to engender their trust.

There is a delicate balance between protecting one's privacy, legitimate business use of personal data, and fraud prevention. However, the use of personal data for fraud prevention and interdiction is beneficial to society. Therefore, fraud and risk management exceptions should be built into any and all laws, regulations, and policies. In fact, the use of personal data for identity theft prevention directly reduces the number of identity theft victims. Further, many industries (i.e. insurance, banking and securities) require fraud prevention through regulation to protect consumers, customers, shareholders, and employees.

Effective authentication in an e-commerce transaction is not possible without the use of independent, personal verification data. Authentication is critical to the growth and confidence of e-commerce.

Fraudsters have quickly learned to defeat our technical systems. If they are allowed to opt out of databases, they will rapidly exploit our vulnerabilities to the financial detriment of the general public.

Global cooperation is also needed in this area. The United States must take a leadership role in fostering cooperation throughout the global community in the development of uniform laws, meaningful and comparable privacy policies, effective assistance to prosecutions by foreign countries, and a sharing of information. The U.S. already has surrendered a leadership role in the areas of privacy and information sharing. The European Union developed a comprehensive privacy directive applicable to all member nations in 1995, and the European Parliament recently refused to allow its member nations to share data and nonpublic information with the U.S. With respect to information sharing, Interpol has announced its intention to provide private industries throughout the world with intelligence information regarding the vulnerability of those industries or specific companies to cyber attacks. At this point, the global community perceives the U.S. as a reluctant partner, not a leader.

Global Interaction and Cooperation

For the past two decades, the international community has focused on the development of extradition treaties, mutual legal assistance treaties, and sanctions to combat the proliferation of money laundering crimes on an international scale. The international focus for the next two decades must be directed toward Internet crime and cyber crime. That focus cannot be limited to procedural remedies. Many countries lack substantive laws specifically designed to combat computer and Internet crimes. For example, the alleged perpetrators of the "Love Bug" virus in the Philippines could not be charged with a substantive crime because no computer crime laws had been enacted in that country. The international community must maintain a more aggressive and comprehensive approach to cyber crime, including treaties that provide for uniform laws on cyber crime and cyber terrorism. That approach should be inspired and led by the United States.

On April 27, 2000, the Council of Europe released a draft version of its proposed International Convention on Cyber-Crime. In 1989 and 1995, the Council encouraged member governments to revise or adopt laws specific to the challenges of computer crime. However, a binding legal agreement is now considered necessary to harmonize computer crime laws and to step up investigations and ensure effective international cooperation. The Council hopes to adopt the Convention by September 2001.

The Convention draft requires each signatory nation to adopt legislation or other measures with respect to five categories of crimes:

- Offenses against computer data and systems;
- Computer-related forgery;
- Computer-related fraud;
- Child pornography; and
- Copyright and intellectual property offenses.

The Convention draft also contains uniform provisions for searches and seizures of computers and computer data, extradition, and mutual legal assistance procedures. The United States has participated in the negotiations preliminary to the release of the Convention draft. The Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice assisted in the drafting process. U.S. government agencies, including the Department of Justice, plan to seek legislative support for the Convention.

In addition, the Group of Eight (G8) nations have discussed economic crime and cyber crime during recent annual summits in London and Moscow. The issue again appeared on the summit agenda for the July meeting in Okinawa. CCIPS chairs the G8 subgroup on high-tech crime. The OECD has made recommendations for industry and government to work together in order to combat money laundering. Guidelines have been established for authentication and "know your customer programs".

Congress needs to address, both from a domestic and global perspective, current law enforcement tools that are needed for investigations and prosecutions in the digital environment. Although Congress has enacted laws that facilitate global e-commerce, for example, the Electronic Signature in Global and National Commerce Act, it has not considered legislation focusing upon the investigation and enforcement of crimes committed in the e-commerce venue. For example, law enforcement needs judicial guidance, but preferably legislative authorization, regarding the search and seizure of computers and peripheral equipment, eavesdropping with new technological devices, and the preservation and presentation of digital evidence. Without Congressional initiative, state and federal courts will continue on a path of conflicting decisions that inhibit effective law enforcement investigations and effectively paralyze U.S. cooperation with foreign governments.

VIII. Conclusion: Trends and Observations

According to the National White Collar Crime Center's *National Public Survey on White Collar Crime*, FBI statistics indicate that, for the period from 1988 to 1997, arrests for violent crimes decreased, but the arrest rate for crimes having to do with fraud and embezzlement increased dramatically.[47] As is evident from this study, this trend is sure to continue, and to grow, as technology facilitates the emergence of cyber crime. As a result of the burgeoning of e-commerce, cyber crime has become prevalent, and it will soon be difficult to differentiate among traditional economic and cyber crimes.

Reporting of economic and cyber crime is problematic and grossly underestimated, as is apparent from the reluctance of corporations to report fraud losses and activity. The FBI's Uniform Crime Report should be revised to include specific economic crimes, following the Fraud Identification Codes established by the National Fraud Center. Until such a means of reporting is implemented and the stigma of fraud victimization is removed, this problem will not be solved. Uniform and thorough reporting is necessary in the war on economic and cyber crime; resources for investigation and prosecution will naturally follow as the enormity of the problem unfolds.

Preventing, detecting, investigating, and prosecuting economic crimes must become a priority, in order to lessen their impact on the economy and the public's confidence. Law enforcement, as it stands now, is in danger of slipping further behind the highly sophisticated criminals. New resources, support for existing organizations, e.g. The National Fraud Center, The National White Collar Crime Center, The Internet Fraud Council, and The Economic Crime Investigation Institute, and innovative solutions are needed to control this growing problem in America and the world.

This is not to say that the focus should be entirely on economic crime to the detriment of investigation and prosecution of violent crime. Certainly, it would not be in society's best interest to have violent crime increase, while economic crime decreases. However, it has often been questioned and argued whether the psychological and financial impact of economic crime on its victims is as great or greater in many instances as violent crime. Rather, higher priority must be given to the provision of necessary resources and the passage of relevant legislation to counter the near-epidemic impact of economic crime on American society and the world.

This can only be accomplished with the cooperation of the private, public, and international sectors. All stakeholders must be more willing to exchange information on the effect economic and cyber crime has on them and the methods they are using to detect and prevent it. No one sector holds all the resources, tools or solutions. In fact, in many instances, industry has more

resources than government, but must be motivated and authorized to partner and communicate. All parties must be willing to work together to effect change in existing laws and regulations and to promulgate new initiatives. The "victims" need to follow the lead of the "criminals" and organize themselves, so that the organized "bad guys" are not operating in a lawless environment, where culpability is at a minimum.

---

1 www.nationalfraud.com

2 Ibid.

3 http://www.ckfraud.org/statistics.html (August 2, 2000)

4 Marjanovic, Steven. "Citigroup Bulks Up Check-Fraud Defense," American Banker, June 23, 2000, 165: 121, p. 12.

5 http://www.ozemail.com.au/~born1820/mlmethod.htm

6 Financial institutions are defined in the Gramm-Leach-Bliley Act as, " Any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956." 15 U.S. C. § 6805 (3) (A). The allowed financial activities of such institutions are set forth in 12 U.S.C. § 1843 (4).

7 PR Newswire. "ShopNow.com Unveils PCCharge Transaction Processing Alliance, an Innovation in Credit Card Fraud Protection", March 8, 2000.

8 Trombly, Maria. "VISA program to Fight Online Fraud Debuts," Computerworld. July 24, 2000, p. 42.

9 Rivera, Elaine. "Dirty Little Diagnosis?" Time. February 7, 2000, 155:5, p. 1c.

10 http://www.fbi.gov/programs/fc/ec/about/about_if.htm (August 2, 2000)

11 http://www.senate.gov/~appropriations/commerce/testimony/levitt.htm (August 2, 2000)

12 Ibid.

13 www.treas.gov/usss/financial_crimes.htm (July 8, 2000).

14 www.beckcomputers.com/articles/wpapers/howbig.htm (Nov. 13, 1998).

15 http://www.wirelessweek.com/news/june00/nine65.htm (August 2, 2000)

16 Mason, Charles. "Cellular/PCS Carriers Continue to Weather Losses from Fraud," America's Network., Feb. 1999, 103:2, p. 18

17 Ibid.

18 http://www.ftc.gov/speeches/thompson/japan22.htm (August 2, 2000)

19 http://www.aarp.org/fraud/1fraud.htm (August 2, 2000)

20 Hazlewood, Sara. "Tech Firms Watching Trade Secret Trials," Business Journal Serving San Jose & Silicon Valley, May 14, 1999, 17:2, p. 7.

21 http://www.privacyrights.org/ar/wcr.htm (August 2, 2000)

22 http://cjonline.com/stories/011900/leg_idtheft.shtml (August 2, 2000)

23 Pfister. "Be on the Lookout for ID Thieves," Denver Business Journal, October 1, 1999, 51:6, p. 13A.

24 Sutherland, Edwin H. White Collar Crime. NY: Dryden Press, 1949.

25 Gordon, Gary. "The Impact of Technology-Based Crime on Definitions of White Collar/Economic Crime: Breaking Out of the White Collar Crime Paradigm." In J. Helmkamp et. al. (eds.). Proceeding of the Academic Workshop: Can and Should There Be a Universal Definition of White Collar Crime? Morgantown, WV: National White Collar Crime Center, 1996.

26 18 U. S. C. § 1030

27 Those states that have enacted identity theft statutes are as follows:

Arizona	Ariz. Rev. Stat. § 13-2708
Arkansas	Ark. Code Ann. § 5-37-227
California	Cal. Penal Code § 530.5
Connecticut	1999 Conn. Acts 99
Georgia	Ga. Code Ann. §§ 121-127
Idaho	Idaho Code § 28-3126
Illinois	720 ILCS 5/16G
Iowa	Iowa Code § 715A8
Kansas	Kan. Stat. Ann. § 21-4108
Maryland	Md. Ann. Code art. 27 § 231
Massachusetts	Mass. Gen. Laws ch. 266 § 37E
Mississippi	Miss. Code Ann. § 97-19-85
Missouri	Mo. Rev. Stat. § 570.223
New Jersey	N.J. Stat. Ann. § 2C:21-17
North Dakota	N.D.C.C. § 12.1-23-11
Ohio	Ohio Rev. Code Ann. 2913
Oklahoma	Okla. Stat. tit. 21, § 1533.1
Tennessee	Tenn. Code Ann. § 39-14-150
Texas	Tex. Penal Code § 32.51
Washington	Wash. Rev. Code § 9.35
West Virginia	W. Va. Code § 61-3-54
Wisconsin	Wis. Stat. § 943.201

28 Linda Rosencrance, "News-Early" section, ComputerWorld, July 24, 2000, p. 20.

29 "Warrants for Online Data Soar," USA Today, July 28, 2000, p. 1A.

30 See the proposed Security and Freedom Through Encryption (SAFE) Act of 1999, H.R. 850.

31 H.R. 4403, § 3 (a).

32 Bass, Roland and Lois Hoeffler, Telephone Based Fraud: A Survey of the American Public. New York: Louis Harris and Associates, 1992.

33 American Association of Retried Persons, Findings from a Baseline Omnibus Survey on Telemarketing Solicitation. Washington, DC: AARP, 1996.

34 Rebovich, Donald et. al. The National Public Survey on White Collar Crime. Morgantown, WV; National White Collar Crime Center, 2000.

35 Ibid.

36 Ibid.

37 www.nationalfraud.com (August 3, 2000)

38 Hazlewood, Sara. "Tech Firms Watching Trade Secret Trials," Business Journal Serving San Jose & Silicon Valley, May 14, 1999, 17:2, p. 7.

39 www.senate.gov/`thompson/pr012600.html (August 3, 2000)

40 http://www.msnbc.com/news/427628.asp (July 3, 2000); http://www.bbc.co.uk/low/english/sci/tech/newsid_812000/812764.stm (June 30, 2000).

41 www.nationalfraud.com (August 3, 2000)

42 www.ecii.edu/about_mission.html (August 3, 2000)

43 http://www.nw3c.org/vision.htm (August 3, 2000)

44 http://www.internetfraudcouncil.org/ (August 3, 2000)

45 ibid.

46 http://www.fbi.gov/programs/carnivore/carnivore2.htm (August 3, 2000)

47 Rebovich, Donald et. al.