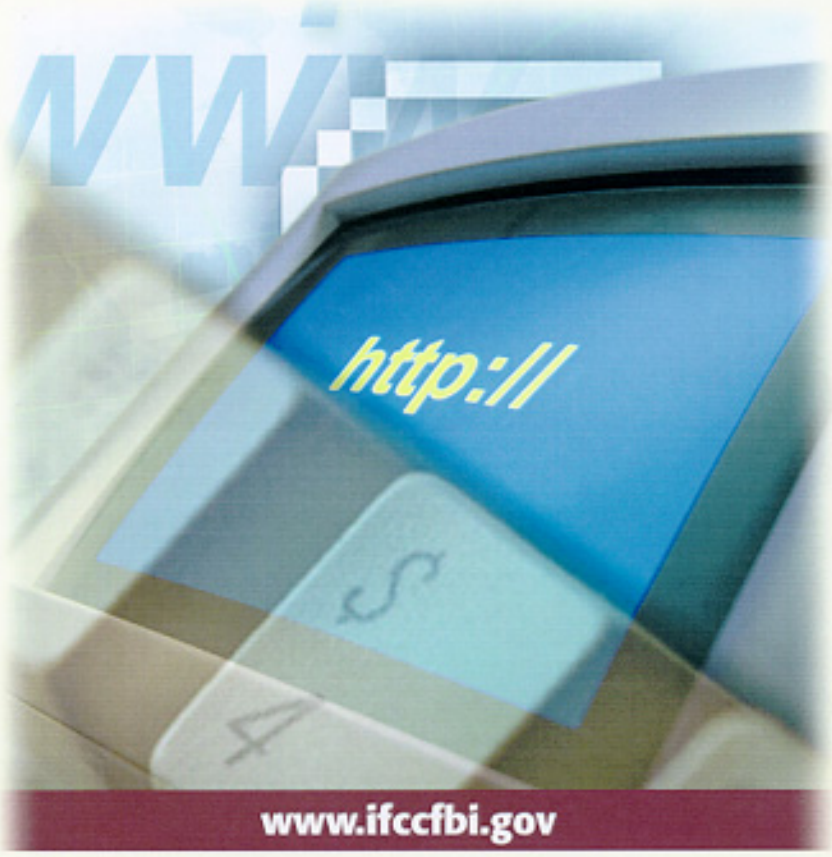
IFCC

Internet Fraud Complaint Center



www.ifccfbi.gov

NW3C

NATIONAL WHITE COLLAR CRIME CENTER

Internet Fraud Complaint Center
(IFCC)

TABLE OF CONTENTS

IFCC

Internet Fraud Complaint Center

NW3C

NATIONAL WHITE COLLAR CRIME CEN

Welcome to IFCC

Welcome to the 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).

NW3C

Fight back with IFCC

IFCC's mission is to address fraud committed over the Internet. For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation. For law enforcement and regulatory agencies at all levels, IFCC offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.

To visit the IFCC site map, click here.

This program is brought to you by the Federal Bureau of Investigation and the National White Collar Crime Center.

INTERNET FRAUD COMPLAINT CENTER

INTERNET FRAUD

One of the most critical challenges facing the FBI and law enforcement in general, is the use of the Internet for criminal purposes. Understanding and using the Internet to combat Internet fraud is essential for law enforcement. The fraud being committed over the Internet is the same type of white collar fraud the FBI has traditionally investigated but poses additional concerns and challenges because of the new environment in which it is located. Internet fraud is defined as any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms, and E-mail, play a significant role in offering nonexistent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices, or other items of value to the control of the scheme's perpetrators. The frauds range from simple geometric progression schemes to complex frauds. The Internet appears to be a perfect manner to locate victims and provides an environment where the victims don't see or speak to the fraudsters. Anyone in the privacy of his or her own home can create a very persuasive vehicle for fraud over the Internet. In addition, the expenses associated with the operation of a "Web site" and the use of electronic mail (E-mail) are minimal. Fraudsters do not require the capital to send out mailers, hire people to respond to the mailers, finance and operate toll free numbers, etc. This technology has evolved exponentially over the past few years and will continue to evolve at a tremendous rate. The accessibility of such an immense audience coupled with the anonymity of the subject, require a different approach.

SITUATION

Computer crimes can be broken down into two main categories: computers used as targets where the general motivation is to impair, damage or alter the computer system; or when the computer merely serves to facilitate the illegal activity. Computer facilitated crimes are those criminal activities that use computers as a way to commit a host of crimes.

Internet fraud does not have traditional boundaries as seen in the traditional schemes. No one knows the full extent of the fraud being committed on the Internet. Not all victims report fraud, and those who do, do not report it to one central repository.

One of the most critical problems associated with fraud being perpetrated over the Internet is the fact that the instances of fraud are disjointed and spread throughout the country. The traditional methods of detecting, reporting, and investigating fraud fail in this environment. Victims of fraud are unsure of how or where to report what they see or what they have experienced on the Internet. Law enforcement agencies receive complaints in a piecemeal fashion, most not reaching a level to advance the complaint to an investigation. Another problem is venue. Complaints are often misdirected and lost due to the fact that the Internet is virtual as

opposed to physical. Without some technical investigatory steps it is usually impossible to identify the location of a Web site or the origin of an E-mail.

Computer facilitated financial scams perpetrated via the Internet and the theft of technology and/or intellectual property by competitors, foreign intelligence services, or those merely seeking personal gain are rapidly growing. Internet related and computer facilitated crimes, primarily impact the priority White Collar Crime (WCC) problem areas of financial institution fraud, securities and commodities fraud, telemarketing fraud, money laundering, insurance frauds, and theft of technology/intellectual property rights.

SECURITIES/COMMODITIES FRAUD

Securities offered over the Internet have added an entirely new dimension to securities fraud investigations. Investors are able to research potential investments and invest over the Internet with ease through electronic linkage to a number of services that provide stock and commodity quotations, and critical financial information. Both the low cost of setting up a Web site and the anonymity available, have made the Internet especially vulnerable to crime. The Internet has helped democratize the investment process by providing widespread access to the most specialized information, giving the appearance to thousands of investors of having an equal access to what was otherwise difficult to obtain data. There is a growing problem with chat rooms, E-mail messages sent en masse (spams), and newsletters that provide fraudulent information related to publicly traded stocks. The North American Securities Administrators Association has estimated that Internet-related stock fraud is currently the second most common form of investment fraud resulting in an estimated $10 billion per year (or $1 million per hour) loss to investors.

The Office of Internet Enforcement-Securities and Exchange Commission (OIE-SEC) was recently established to focus on securities fraud, particularly as it relates to solicitations of securities utilizing the Internet. The new SEC branch continues to receive numerous referrals from the general public regarding these Internet frauds. After culling the referrals, as a matter of policy, the SEC would generally make direct contact with the firms that may be perpetrating fraud on the Internet. The FBI has had an ongoing cooperative relationship with the SEC, and recent collaborative efforts have solidified both agencies= desire to identify and combat securities fraud over the Internet. Securities fraud leads originating from the Internet that may be presented to the FBI by OIE-SEC and other outside sources include micro-cap stock fraud, prime bank note schemes, schemes involving investment contracts Aguaranteeing@ results, Ponzi schemes, foreign currency exchange schemes, and fraudulent unregistered initial offering matters.

MONEY LAUNDERING/ CYBERLAUNDERING

Cyberpayments

The term cyberpayments is just one of many used to describe systems which facilitate the transfer of financial value. Other terms include digital currency and E-cash. These developments may alter the means by which all types of financial transactions are conducted and financial payments systems are operated. This new technology will change many of the fundamental principles associated with a "cash" oriented society. Such transactions may occur via the Internet or through the use of "smart cards" which, unlike debit or credit cards, actually contain a microchip which stores value on the card. The common element is that these systems are designed to provide the transacting parties with immediate, convenient, secure and potentially anonymous means by which to transfer financial value. Although these systems will provide readily apparent benefits to legitimate commerce, it may also have the potential to facilitate the international movement of illicit funds. These same reasons impede law enforcement from obtaining necessary information to detect illegal activity.

Smart Cards

Smart Cards or stored value cards will make it easier for the money launderer to transfer illicit funds without detection by law enforcement and financial institutions. Because the cash value is stored on the card, there is no need for the merchant to dial up a bank or credit card company to get approval. Users can add cash values at machines and a person may hold numerous cards.

Cyberlaundering

Cyberlaundering is the latest technique in money laundering. Money laundering was a physical transportation of hard cash to conceal the existence, illegal source or illegal application of income and then disguising the income to make it appear legitimate. As the physical world of money laundering began to erode, the tendency to use electronic transfers (wire transfers) to avoid detection gained a loyal following. The wire transfer system allows criminal organizations, as well as legitimate businesses and individual banking customers to enjoy a swift and nearly risk-free conduit for moving money between countries.

In the virtual universe of cyberspace, the demand for efficient consumer transactions has lead to the establishment of electronic cash. E-cash or digital money, is an electronic replacement for cash. Digital cash has been defined as a series of numbers that have an intrinsic value in some form of currency. Using digital cash, actual assets are transferred through digital communications in the form of individually identified representatives of bills and coins - similar to serial numbers on hard currency. Digital transfers are anonymous. Even if the cyberbanks that accept anonymous E-cash are somehow subject to the same laws and regulations that financial institutions in the tangible world are, the launderer must first be caught. The reports will be virtually useless, as the banks have no knowledge as to which funds are the launderer's. This provides for anonymous money laundering. Structuring of transactions so as to avoid currency-reporting requirements becomes less risky if the funds used to structure are virtually untraceable. In addition, the filing of currency transaction reports may be pointless if the money can not be

traced into a specific account. However, the actual requirement that a transaction report be filed may be nonexistent if cyberbanks that accept E-cash deposit accounts do not fall under current federal or state regulation of financial institutions.

FINANCIAL INSTITUTION FRAUD/CYBERBANKING

In order to remain competitive and provide a broader product line, financial institution mergers and acquisitions are common place. The market is even experiencing banks merging with insurance companies (CitiBank and Travelers Insurance). In order to better serve their customers and reduce costs, banks are offering Internet-based one stop financial shopping supermarkets. These systems include electronic bill payment/presentation services, financial planning, securities trading, and insurance. The implementation of information technologies in the financial services industry ties traditional bank frauds such as commercial loan fraud, check fraud, counterfeit negotiable instruments, mortgage fraud, check kiting, and false applications with insurance fraud, securities fraud, and computer fraud and abuse. The American Bankers Association and the banking industry at large have identified cyberbanking, the use of emerging technologies, and the associated related fraud as an area to focus on. They have also identified mergers as an opportunity for fraud given the vulnerability of the merging computer systems.

TELEMARKETING FRAUD

The National Consumer League's Internet Fraud Watch (IFW) reported for 1999, the ten most frequently reported types of Internet frauds: (1) online auctions (by far the most frequently reported scheme); (2) general merchandise sales; (3) Internet services; (4) computer equipment and software; (5) work-at-home schemes; (6) advance fee loans; (7) magazines; (8) adult services; (9) travel/vacations; and (10) pyramid/multi-level marketing schemes. The IFW program received 7,439 reports of fraud in 1998, and in 1999 the complaints increased to 10,660, averaging approximately 890 per month.

Many of these types of frauds are identical to the types of frauds that are conducted through telemarketing operations. Indeed, law enforcement authorities report that a number of Internet-related schemes are set up to induce prospective victims, through the use of the Internet (e.g., by creating a Web site falsely promising get-rich-quick opportunities), to call toll-free numbers where telemarketers can present their pitches and persuade them to send money.

BANKRUPTCY FRAUD

The most common types of bankruptcy schemes on the Internet involve petition mills, equity skimming, and credit repair operations. Petition Mills/Equity Skimming schemes are the fastest growing and most pervasive areas of bankruptcy fraud throughout the nation. The perpetrators target individuals in foreclosure, eviction, or other financial distress and offers them a "too good to be true" solution to their problems. The victims are instructed to pay their rent or mortgage payments to the perpetrator based on the promise that the perpetrator will deal with

their creditors and resolve the foreclosure/eviction proceedings. Usually without the victim=s knowledge, the perpetrator files a bankruptcy case in the victim=s name to take advantage of the automatic stay. When collection efforts cease because of the filing, the victim believes his financial problems are being addressed and continues to pay the perpetrator.

INSURANCE FRAUD

The most common types of insurance schemes on the Internet involve surety bonds, phony union memberships, and providing fraudulent insurance coverages. These fraudulent insurance operations will use the Internet as a marketing tool to attract businesses/individuals and will provide information, a contact telephone number and information about the services they can provide.

THEFT OF TECHNOLOGY/INTELLECTUAL PROPERTY RIGHTS (IPR)

The Internet and digital technology have provided an unprecedented means for criminals to not only profit from the theft of intellectual property, but also permanently diminish its value in the process. The United States is the world leader in the development of creative, technical and intellectual products. These products have essentially supplanted tangibles such as steel and wheat as our economic lifeblood. Many of these industries have a direct and tangible impact on the economic well being of the U.S. According to the International Intellectual Property Alliance, copyright piracy cost an estimated loss of $10.8 billion to U.S. copyright industries. A rapidly growing majority of all IPR violations are now Internet based. Tens of thousands of Web sites are solely designed to distribute pirated material. The potential damage to U.S. Intellectual Property owners from this form of theft is escalating daily. Currently, industry groups such as the Business Software Alliance (BSA) and Software Publishers Association (SPA) actively search out piracy sites. Once identified, BSA or SPA attempts to shut down piracy sites by contacting the infringing site=s Internet Service Provider (ISP) to have the site taken off the Web. Often times such sites simply reappear on another ISP weeks later. In other instances, these groups may attempt to pursue civil remedies, but more often than not, this too is ineffective. Without law enforcement authority, these rights holders are left powerless to protect their valuable works from theft.

The IFW study did not report on securities-related investment schemes on the Internet, largely because the Securities and Exchange Commission (SEC) has its own on-line complaint center for reporting possible Internet securities frauds. The SEC=s own data show that as smaller investors continue to show intense interest in purchasing any kind of Internet-related stock,[1]

[1] A series of initial public offerings (IPOs) by Internet companies in the fall of 1998 exemplified what one analyst called the Internet feeding frenzy by investors. On the day that they went public, companies such as Theglobe.com (a fledgling company that helps people design Web sites) and E-Bay (an online auction service) had 606 % and 163 % increases, respectively, from their offering prices to their first-day closing prices. Theglobe.com=s gain was the best first-day performance of any IPO, excluding the very smallest

securities fraud through the Internet is also a growing concern. The SEC reportedly receives 120 complaints a day from online investors about Internet-related securities schemes.[2] Many of the Internet-related schemes that the SEC has pursued through enforcement actions have obtained millions, and in some cases, tens of millions of dollars in investor funds.[3] This reinforces the fact that the above charts contain only a portion of the overall crime problem on the Internet. From all available evidence, electronic commerce on the Internet (E-commerce) is beginning a tremendous surge in growth. One of the leading Internet research companies has recently predicted that U.S. business trade on the Internet will grow from $43 billion in 1998 to $1.3 trillion in 2003.[4] Another study states that the market for Internet and Internet products and services alone was $49 billion in 1997, and will nearly triple to $142 billion by 2001.[5]

IPOs. The avid buying of such stocks has gone on despite analysts= warnings that the valuations ascribed to many of these companies are highly excessive. Theglobe.com, for example, had $11.5 million in losses on $2.7 million in revenues during the first nine months of 1998, but in mid-November, 1998, had a market value of $622 million. *See* Reed Abelson, Market Place: Webstock >Speculating=, NEW YORK TIMES ON THE WEB, Nov. 16, 1998, <http://nytimes.com/library/tech/98/biztech/articles/16webstocks.html>.

[2] *See*, *e.g.*, Todd Woody, The SEC=s Internet Ranger, INDUSTRY STANDARD, Nov. 16, 1998 <http://www.thestandard.net/articles/article_print/0,1454,2490,00.html>.

[3] *See*, *e.g.*, Gregg Wirth, Policing the Universe, INDUSTRY STANDARD, Nov. 16, 1998 <http://www.thestandard.net/articles/article_print/0,1454,2488,00.html>.

[4] *See* Eye-popping e-commerce numbers, MSNBC, Dec. 17, 1998 <http://www.msnbc.com/news> [Forrester Research Inc.].

[5] *See* "Zona Research Confirms eCommerce Growth, eMarketer<wysiwig://44http://www.emarketer.com/estats/110298_zona.html>.

MISSION STATEMENT

To develop a national strategic plan to address fraud over the Internet and to provide support to law enforcement and regulatory agencies at all levels of government for fraud that occurs over the Internet.

STRATEGY

The development of a proactive strategy to investigate Internet fraud through the establishment of an Internet Fraud Complaint Center (IFCC) as a central repository for complaints is essential. The IFCC is necessary to adequately identify, track, and prosecute new fraudulent schemes on the Internet on a national and international level. IFCC personnel will collect, analyze, evaluate, and disseminate Internet fraud complaints to the appropriate law enforcement agency. The IFCC will provide a mechanism by which the most egregious schemes are identified and addressed through a criminal investigative effort.

The IFCC will provide a central analytical repository for complaints regarding Internet fraud and it will act as a resource for enforcement agencies at all levels of government to include regulatory agencies. It will provide analytical support and aid in the development of a training module to address Internet fraud.

The FBI and the National White Collar Crime Center (NW3C) will cosponsor the IFCC. This partnership will be mutually beneficial for both agencies in that it will allow both agencies to share staffing responsibilities. The IFCC will forward complaints to the appropriate local, state or federal law enforcement agency for investigation. This will ensure that Internet fraud is addressed at all levels of law enforcement.

The IFCC will identify current crime problems and develop investigative techniques to address those newly identified crime trends. The information obtained from the data collected will provide the foundation for the development of a national strategic plan to address Internet fraud and develop ways to lessen the impact of fraudulent activity on the Internet.

GOALS and OBJECTIVES

1. To develop a national strategy to address Internet fraud.

2. To develop criminal Internet fraud cases and obtain criminal prosecutions of those companies and individuals responsible.

3. To prevent the amount of economic loss by Internet fraud throughout the United States.

4. To provide an analytical repository for Internet fraud complaints.

5. To receive, analyze, and refer all fraudulent activity identified on the Internet.

6. To identify current crime trends over the Internet and to develop investigative techniques to address those identified crime problems.

7. To track fraud facilitated by the Internet and provide analytical support of Internet crime trends.

8. To act as an investigative resource for Internet fraud and to develop training modules to investigate Internet fraud.

9. To develop information packets from complaints generated and forward that information to the appropriate law enforcement agencies.

WORK FLOW

Public awareness of the existence and purpose of the IFCC is paramount to the success of this effort. The FBI Web page, which currently receives approximately 25 million hits per month, will accomplish this purpose. A detailed explanation of the complaint center, its purpose and contact numbers will be provided so that consumers can report Internet fraud. The FBI Web page will provide victims with a hyperlink to the IFCC Web page where they can complete a fill-in-the blank complaint form.

Once the complaint is made, it is received by the IFCC personnel for data entry. This constitutes the first screening of the complaint. This first screening's purpose is to receive the information from the complainant which includes name, address, Date of Birth, phone number, Social Security Number, subject company name, Web site, E-mail address, dates of contact, and a brief narrative. In addition, it will serve to notify the complainant that the information will be disseminated by the IFCC to the appropriate enforcement agency. Additionally, if requested by an enforcement agency, the IFCC will provide this information to assist in the furtherance of a criminal or regulatory investigation. The incoming complaint raw data, as initially screened and forwarded to the appropriate database, will be information under the maintenance and control of the NW3C. The complaint information provided will be utilized by the IFCC as the foundation to identify individuals and organizations committing fraudulent acts on the Internet, to identify schemes, and to assist in the identification and recovery of funds.

Once a predetermined number of complaints are received for a particular entity, or the initial complaint merits additional attention, additional inquiries are automatically triggered such as the identification of a Web address, subjects involved, determination of venue and additional background information. The additional inquiries will be from public data bases only. The information developed as a result of the additional inquiries will also be available to enforcement agencies and will be information under the maintenance and control of the NW3C.

When sufficient information has been obtained to establish the possibility of criminal activity, preliminary investigative inquiries will be conducted, to include the utilization of law enforcement data bases, for the purpose of obtaining information to complete the investigative packet. This packet will then be referred to the appropriate law enforcement agency for criminal investigation. This information will be under the maintenance and control of the FBI. The information obtained from these complaints are case sensitive to the law enforcement agency with prosecutive interest only. All local, state and federal law enforcement agencies with jurisdictional interest will receive an investigative packet. It will be those agencies responsibility to coordinate the investigation.

The first level of information will be provided to requesting enforcement agencies. Any information requests on criminal investigation complaints will not divulge existence of an investigation and will only provide the initial complaint information. The investigating law enforcement agency will be notified of the request and be responsible for any follow-up contacts.

All criminal investigative referrals will be tracked to determine the value of the information and the status of investigations.

INTERNET FRAUD COUNCIL WORKING GROUP

IFCC plans to create and solicit participation in an Internet fraud council working group consisting of federal and state law enforcement agencies, federal and state enforcement agencies, and representative of the private sector for the purpose of creating a network to share information, discuss pertinent issues, recommend possible legislative solutions, and maximize the benefit of the IFCC to all enforcement agencies.

OUTSIDE AGENCY PARTICIPATION

Any enforcement agency that desires to participate in the IFCC are welcome and may do so by providing support at the IFA analytical support level. Currently, the Postal Inspection Service and the Internal Revenue Service have analysts at the center.

IFCC PROJECT GOALS

- The development of a national strategic plan to address Internet fraud.
- To provide a mechanism for consumers nationwide to report Internet fraud.
- To provide a reliable analytical repository for Internet fraud complaints identified on the Internet.
- To identify Internet fraud cases.
- To act as a referral base for Internet fraud matters involving criminal, civil and regulatory investigations conducted by local, state and federal agencies.
- To reduce the amount of economic loss by Internet fraud throughout the United States.
- To identify of current crime trends over the Internet, and to development of investigative techniques to address those identified crime problems.
- To act as an investigative resource for Internet fraud, and to develop training modules to investigate Internet fraud.
- The development of web based training for center personnel, which additionally will be used to train law enforcement personnel.
- Receive Internet fraud complaints via the Internet.
- Provides initial screening and forwarding of complaints to a central database.
- The development of an artificial intelligence system to continuously review data received through the online-complaint process.
- Once a predetermined number of complaints are received for a particular subject, analytical steps are initiated.
- Follow-up inquires, such as identification of Web address, subjects involved, venue, and other background information will be obtained, via open source information.
- If the complaint and results of inquiries conducted indicate a criminal investigation is probable, the complaint will be referred to all appropriate local, state and federal enforcement agencies.
- Additional preliminary investigative inquiries are conducted which may include follow-up interviews of the victim and criminal checks.
- An investigative packet is prepared for referral to the appropriate local, state or federal law enforcement agency for criminal investigation.

IFCC ENDORSEMENTS

It should be noted that on May 4, 1999, President Clinton announced the establishment of the IFCC. He stated:

> " We'll also crack down on fraud committed over the Internet. If we want to seize the Internet's full potential, we have to stay ahead of those who would use this open medium to manipulate stock prices, commit fraud in on-line auctions or perpetuate any other type of financial scam. That's why I've asked the Justice Department to step up prosecutions, to develop a national center for tracking Internet fraud, and to train state, local and federal law enforcement officers on how to recognize and root out these schemes.
>
> I find that law enforcement, compared to people who are doing criminal activity in this area, are rather like parents trying to keep up with their children on the computer. It is an endless effort, and we need to organize and systematize a continuous training and retraining effort so that we can stay ahead of the curve."

As stated in the DOJ Internet Fraud Initiative, which was approved by the Attorney General on February 2, 1999:

> " The Initiative would support ongoing efforts between the FBI and the National White Collar Crime Center (NWCCC) to develop a national center for the analysis and strategic use of complaints and other information on Internet fraud schemes. While the Internet Fraud Watch and the FTC have large amounts of Internet fraud-related complaint data, neither organization has the capability to analyze these data to identify possibly criminal schemes and to see that the data are referred to appropriate law enforcement organizations for possible investigation and prosecution. The NWCCC has a $1.5 million appropriation in FY1999 for research and development of a fraud complaint center, and the FBI is now in discussions with the NWCCC to combine FBI and NWCCC resources for analysis and referral of Internet fraud schemes.
>
> Once the FBI and the NWCCC conclude their discussions, the Initiative would work with the FBI and the NWCCC during and after 1999**,** to ensure that the project will generate strategic information that United States Attorneys**'** offices and other federal agencies can use to identify and pursue such schemes on a timely basis. As the Internet Fraud Center gets underway, it can be expected to amass data that can be useful in developing more reliable estimates of the overall size and growth of Internet fraud in all forms."

On May 11, 1999, Eric Holder, the Deputy Attorney General spoke at the Economic Crime Summit in Orlando, Florida. In his remarks, he stated:

> The Department will ensure that federal law enforcement can timely receive and analyze information on internet fraud schemes. The President has directed the Justice Department to establish a national center to pursue Internet fraud, and I am pleased to say that the FBI has joined forces with the National White-Collar Crime Center to establish the Internet Fraud Complaint Center. This new joint venture...will help to ensure that law enforcement and regulators will have timely analysis and strategic information on Internet fraud schemes.

On November 3, 1999, the International Association of Chiefs of Police (IACP) adopted at their 106th Annual Conference a resolution in support for the establishment of the Internet Fraud Complaint Center, they stated:

> The IACP applauds and supports the establishment of the Internet Fraud Complaint Center, a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center, providing a referral and case development mechanism to local, state, and federal enforcement agencies addressing crimes on the Internet.