

U. S. Department of Justice
Federal Bureau of Investigation

FINANCIAL CRIMES SECTION
CRIMINAL INVESTIGATIVE DIVISION

FINANCIAL CRIMES
REPORT TO THE
PUBLIC

FISCAL YEAR 2006
OCTOBER 1, 2005 - SEPTEMBER 30, 2006

TABLE OF CONTENTS

Financial Crimes	A1-A2
Corporate Fraud	B1-B4
Securities and Commodities Fraud	C1-C6
Health Care Fraud	D1-D8
Mortgage Fraud.....	E1-E9
Identity Theft	F1-F5
Insurance Fraud.....	G1-G4
Mass Marketing Fraud	H1-H5
Asset Forfeiture/Money Laundering.....	I1-I4
Acronyms	J1-J2

U. S. Department of Justice
Federal Bureau of Investigation

FINANCIAL CRIMES SECTION
CRIMINAL INVESTIGATIVE DIVISION

FINANCIAL CRIMES

The Federal Bureau of Investigation (FBI) investigates matters relating to fraud, theft, or embezzlement occurring within or against the national and international financial community. These crimes are characterized by deceit, concealment, or violation of trust, and are not dependent upon the application or threat of physical force or violence. Such acts are committed by individuals and organizations to obtain personal or business advantage. The FBI focuses its financial crimes investigations on such criminal activities as corporate fraud, health care fraud, mortgage fraud, identity theft, insurance fraud, mass marketing fraud, and money laundering. These are the identified priority crime problem areas of the Financial Crimes Section (FCS) of the FBI.

The mission of the FCS is to oversee the investigation of financial fraud and to facilitate the forfeiture of assets from those engaging in federal crimes. The FCS is divided into four units: the Economic Crimes Unit, Health Care Fraud Unit, Financial Institution Fraud Unit, and the Asset Forfeiture/Money Laundering Unit.

The Economic Crimes Unit is responsible for significant frauds targeted against individuals, businesses and industries to include: corporate fraud, insurance fraud (non-health care related), securities and commodities fraud, mass marketing fraud, telemarketing fraud, Ponzi schemes, advance fees schemes, and pyramid schemes.

The Health Care Fraud Unit oversees investigations targeting individuals and/or organizations who are defrauding public and private health care systems. Areas investigated under Health Care Fraud include: billing for services not rendered, billing for a higher reimbursable service than performed (upcoding), performing unnecessary services, kickbacks, unbundling of tests and services to generate higher fees, durable medical equipment fraud, pharmaceutical drug diversion, outpatient surgery fraud, and Internet pharmacy sales.

The mission of the Financial Institution Fraud Unit is to identify, target, disrupt, and dismantle criminal organizations and individuals engaged in fraud schemes which target our nation's financial institutions. Areas investigated in the financial institution fraud arena include: financial institution failures, insider fraud, check fraud, counterfeit negotiable instruments, check kiting, loan fraud, and mortgage fraud.

The mission of the Asset Forfeiture/Money Laundering Unit (AF/MLU) is to promote the strategic use of asset forfeiture and to ensure that field offices employ the money laundering violation in all investigations, where appropriate, to disrupt and/or dismantle criminal enterprises.

In addition to these responsibilities, the AF/MLU provides strategy and guidance to field offices as it relates to identity theft across all investigative programs.

The AF/MLU also has responsibilities for the management of the Forfeiture Support Project (FSP) in Calverton, Maryland. Although the FSP's mission is closely tied to that of the AF/MLU, it does have a separate mission statement which is documented as follows: The mission of the FSP is to

support the forfeiture component of all major FBI investigations through data entry and analysis of financial documents, forensic accounting, and tracing assets subject to forfeiture.

Based upon field office crime surveys, current trends in the White Collar Crime arena, and directives established by the President, the Attorney General, and the Criminal Investigative Division, the following national priorities for the White Collar Crime Program have been established: Public Corruption, Corporate Fraud/Securities Fraud, Health Care Fraud, Financial Institution Fraud, Insurance Fraud and Money Laundering.

Although Public Corruption is a national priority within the White Collar Crime Program, it will not be addressed in this report. Each section of this report provides an overview, statistical accomplishments, and case examples of the identified priority crime problems specifically addressed by the Financial Crimes Section. Where appropriate, suggestions are made in order to protect the public from being victimized by fraudulent activity.

CORPORATE FRAUD

I. General Overview

As the lead agency investigating Corporate Fraud, the FBI has focused its efforts on cases which involve accounting schemes, self-dealing by corporate executives and obstruction of justice. The majority of Corporate Fraud cases pursued by the FBI involve accounting schemes designed to deceive investors, auditors and analysts about the true financial condition of a corporation. Through the manipulation of financial data, the share price of a corporation remains artificially inflated based on fictitious performance indicators provided to the investing public. In addition to significant financial losses to investors, Corporate Fraud has the potential to cause immeasurable damage to the U.S. economy and investor confidence.

While the number of cases involving the falsification of financial information remains relatively stable, the FBI has recently observed a spike in the number of Corporate Fraud cases that involve the backdating of executive stock options. Stock options are corporate incentives that allow the holder to purchase stock at a fixed "strike" price sometime in the future, regardless of the prevailing market price. Generally, the strike price is the cost of the stock on the date the options were granted. The benefit to the options holder is the difference between the strike price and the later sales price. When stock options are backdated, however, the date of the options is set to a time in the past when the price of the stock was lower than on the date the options were actually issued. Backdating stock options inflates their value to the holder at the expense of regular shareholders. Some corporate executives have also changed their stock option exercise date (the date the option can be converted to stock) to avoid paying income tax. Currently, the FBI is investigating 59 cases involving the manipulation of executive stock options and anticipates that the number of cases will continue to grow.

Corporate Fraud remains the highest priority of the Financial Crimes Section and the FBI is committed to dealing with the significant crime problem. As of the end of Fiscal Year (FY) 2006, 490 Corporate Fraud cases are being pursued by FBI field offices throughout the U.S., 19 of which involve losses to public investors that individually exceed \$1 billion.

Corporate Fraud investigations involve the following activities:

(1) Falsification of financial information, including:

- (a) False accounting entries
- (b) Bogus trades designed to inflate profit or hide losses
- (c) False transactions designed to evade regulatory oversight

(2) Self-dealing by corporate insiders, including:

- (a) Insider trading

- (b) Kickbacks
- (c) Backdating of executive stock options
- (d) Misuse of corporate property for personal gain
- (e) Individual tax violations related to self-dealing

(3) Fraud in connection with an otherwise legitimately-operated mutual or hedge fund:

- (a) Late trading
- (b) Certain market timing schemes
- (c) Falsification of net asset values
- (d) Other fraudulent or abusive trading practices by, within, or involving a mutual or hedge fund

(4) Obstruction of justice designed to conceal any of the above-noted types of criminal conduct, particularly when the obstruction impedes the inquiries of the Securities and Exchange Commission (SEC), other regulatory agencies, and/or law enforcement agencies.

The FBI has formed partnerships with numerous agencies to capitalize on their expertise in specific areas such as Securities, Tax, Pensions, Energy, and Commodities. The FBI has placed greater emphasis on investigating allegations of these frauds by working closely with the SEC, National Association of Securities Dealers (NASD) Regulation, Internal Revenue Service (IRS), Department of Labor, Federal Energy Regulatory Commission, Commodity Futures Trading Commission (CFTC) and U.S. Postal Inspection Service (USPIS). As reflected in the statistical accomplishments of the Presidential Corporate Fraud Task Force (founded 2002), which includes the above-mentioned agencies, the cooperative and multi-agency investigative approach has resulted in highly successful prosecutions

The FBI has also worked with numerous organizations in the private industry to increase public awareness about combating Corporate Fraud, to include: Public Company Accounting Oversight Board, American Institute of Certified Public Accountants and the North American Securities Administrator's Association, Inc. These organizations have been able to provide referrals for expert witnesses and other technical assistance regarding accounting and securities issues. In addition, the Financial Crimes Enforcement Network (FinCEN) and Dunn & Bradstreet have been able to provide significant background information on subject individuals or subject companies in an investigation.

II. Overall Accomplishments

During FY 2006, the FBI investigated 490 Corporate Fraud cases resulting in 171 indictments and 124 convictions of corporate criminals. Numerous cases are pending plea agreements and trials. The following notable statistical accomplishments are reflective in FY 2006 for Corporate Fraud: \$1.2 billion in Restitutions, \$41.5 million in Recoveries, \$14.2 million in Fines, and \$62.6 million in Seizures. The chart below is reflective of the number of pending cases from FY 2002 through FY 2006.

III. Significant Cases

COMVERSE, INC. (NEW YORK):

Comverse, Inc. (Comverse) is a New York-based designer and manufacturer of telecommunication systems and software, with reported revenues of \$1.2 billion in FY 2005. In August 2006, former Comverse Chief Executive Officer Kobi Alexander, former Chief Financial Officer David Kreinberg, and former General Counsel William Sorin were charged with various types of fraud related to illegal compensation of Comverse executives. It is alleged that Comverse rewarded certain executives of the company through Executive Stock Option (ESO) backdating, a process that allows executives to set the grant date of the ESO at a time in the past when the market price of the stock was at its lowest. It is alleged that Alexander made \$8 million, Kreinberg \$1.5 million, and Sorin more than \$1 million from the scheme. Kreinberg and Sorin surrendered to authorities in August 2006. As of December 1, 2006, Alexander is in the custody of law enforcement officials in the country of Namibia pending extradition to the U.S. The FBI conducted this case with assistance from the SEC and Department of Justice (DOJ).

ENRON CORPORATION (WASHINGTON, DC):

As a result of its deceptive accounting practices--including the creation of earnings, the manufacture of cash flow, and the concealment of debt--the Enron Corporation (Enron) generated financial statements that were misleading and wholly inaccurate. As of December 1, 2006, 35 individuals have been charged in connection with the energy corporation's illegal accounting practices. Of these individuals, 23 have pled guilty or been convicted, including former Enron Chief Financial Officer (CFO) Andrew Fastow, former Chief Executive Officer (CEO) Jeffrey Skilling, and former Chairman and CEO Kenneth Lay (whose conviction was later vacated due to his death). Fastow has been sentenced to six years in prison for his role in the accounting scandal. Skilling was sentenced to 24 years, four months in prison, the largest term handed down in connection to the case. The case has been handled by the Enron Task Force, which is made up of members of the DOJ, FBI, and IRS. The SEC also provided considerable assistance in this investigation.

U. S. Department of Justice
Federal Bureau of Investigation

FINANCIAL CRIMES SECTION
CRIMINAL INVESTIGATIVE DIVISION

SECURITIES AND COMMODITIES FRAUD

I. General Overview

With losses totaling approximately \$40 billion per year, combating Securities and Commodities Fraud remains a priority for the FBI. The losses are associated with decreased market value of businesses, reduced or non-existent return on investments, and legal and investigative costs. The victims of Securities and Commodities Frauds include individual investors, financial institutions, public and private companies, government entities, and retirement funds. As of FY 2006, the FBI is investigating 1655 cases of Securities and Commodities Fraud and has 157 agents dedicated to the problem. The importance of this issue is further evidenced by the fact that these 157 agents represent a 25 percent increase in staffing for this type of fraud over the last two years.

Whether through college savings plans or retirement accounts, more and more Americans are choosing to invest in the U.S. securities and commodities markets. In fact, the Securities and Exchange Commission (SEC) suggests that the number of people investing in securities and commodities has increased 600 percent since 1980. This large scale investment growth, however, has also led to significant growth in the amount of fraud and misconduct seen in these markets.

The nation's economy is increasingly dependent on the success and integrity of the securities and commodities markets. As a result, there is a very real need to diligently prosecute criminal activity in the markets, which the FBI is uniquely positioned to investigate. In an effort to meet this need, the FBI remains committed to investigating and preventing all forms of Securities and Commodities Fraud, the most common types of which are outlined below.

Market Manipulation: Market Manipulation or "Pump and Dump" schemes are based on the manipulation of lower-volume stocks purchased on small over-the-counter markets. The basic goal of Market Manipulation fraud is to artificially inflate ("pump") the price of penny stocks so that the conspirators can sell ("dump") their shares at a large profit. The "pump" involves recruiting unwitting investors through false or deceptive sales practices, public information, or corporate filings. Many of these schemes use "boiler room" methods where brokers, who are bribed by the conspirators, use high pressure sales tactics to increase the

number of investors and therefore raise the price of the stock. Once the price of the targeted shares reaches a certain point, the perpetrators "dump" their shares at a huge profit and leave innocent investors to foot the bill. These schemes generate an estimated \$6 billion in losses each year and have the ability to significantly impact investor confidence.

One recent trend seen in Market Manipulation cases involves "computer intrusion." Computer intrusion for the purpose of Market Manipulation often includes a criminal hacking into victims' personal online brokerage accounts and using them to purchase shares of a penny stock to inflate its price. As in normal "Pump and Dump" schemes, once the price of the stock reaches a certain

point, the perpetrators dump their own shares and walk away with a large profit.

High Yield Investment Fraud: High Yield Investment Fraud schemes can take many forms, all of which are characterized by offers of low risk investments that guarantee an unusually high rate of return. Victims are enticed by the prospect of easy money and a fast turnaround.

One common form of these frauds is the Ponzi Scheme, which is named after early 20th century criminal Charles Ponzi. These schemes use money collected from new victims, rather than profits from an underlying business venture, to pay the high rates of return promised to earlier investors. This arrangement gives investors the impression that there is a legitimate, money-making enterprise behind the fraudster's story, but in reality, unwitting investors are the only source of funding.

Pyramid Schemes are another common form of High Yield Investment Fraud. In Pyramid Schemes, as in Ponzi Schemes, money collected from new participants is paid to earlier participants. In Pyramid Schemes, however, participants receive commissions for recruiting new participants into the scam.

Another type of High Yield Investment Fraud is Prime Bank Investment Fraud. In these schemes, victims are told that certain financial instruments (notes, letters of credit, debentures, or guarantees) have been issued by well-known institutions such as the World Bank and offer a risk-free opportunity with high rates of return. Perpetrators often claim that the unusually high rates of return and low risk are the result of a worldwide secret exchange open only to the world's largest financial institutions. Victims are often drawn into Prime Bank Investment Frauds because the criminals use sophisticated terms, legal looking documents, and claim that the investments are insured against loss.

Advanced Fee Schemes: In these scams, victims are persuaded to advance relatively small sums of money in the hope of realizing a much larger gain. In Securities Fraud, victims are told that in order to have the opportunity to be an investor in an initial offering of a promising security, investment (business or land development) or commodity, the victim must first send funds to cover taxes or processing fees. Advanced Fee schemes are further defined in the Mass Marketing Section of this report.

Hedge Fund Fraud: Hedge Funds (HFs) are private investment partnerships that routinely accept only high-wealth clients willing to invest at least hundreds of thousands of dollars. Historically, these high wealth investors were deemed "financially sophisticated," and, as a result, HFs have been unregulated and are not required to register with any federal or state regulatory agency. More recently, many middle class investors have been exposed to HFs through ancillary investments such as pensions and endowments. There are over 8,800 HFs currently operating, with over \$1.3 trillion in assets under management.

The lack of regulatory scrutiny has made the industry vulnerable to fraud by HF managers. The types of fraud associated with HFs include: overstatement of HF assets, misappropriation of assets, miscalculation of HF manager performance fees, trading on insider information, market timing, and late trading.

Commodities Fraud: Commodities fraud is perpetrated by firms or individuals that sell futures

and options through illegal means. For example, investments in precious metals or commodities may be sold based on fraudulent sales pitches claiming high rates of return, with little risk, if clients purchase commodities through a financing agreement. Sometimes the perpetrators will offer the opportunity to speculate on movements in the price of commodities, without ever actually taking delivery of the commodity. Traders may also illegally manipulate the price of a commodity. In these cases, the traders report fraudulent pricing information or corner-the-market on certain commodities in order to inflate the price for their profit.

Foreign Currency Fraud: The perpetrators of these frauds are foreign currency trading firms that entice individuals into investing in the spot foreign currency (Forex) market by false claims and high pressure sales tactics. Additionally, individual currency traders employed by large financial institutions may manipulate Forex prices and divert profit to themselves. Corrupt currency trading firms use fraudulent sales practices including false and deceptive guarantees of future return on investment. These firms may even create artificial account statements that reflect a purported investment in the Forex market when, in reality, no such investment has been made. When the currency trading firms actually invest clients' funds into the Forex market, they do so not with intent to conduct a profitable trade for the client, but merely to "churn" the client's account. Churning creates large commission charges benefitting the trading firm at the expense of the client's interests.

Broker Embezzlement: Investors and corporations must place a significant amount of trust in their brokers because these individuals have access to information related to their clients' personal or corporate wealth. Unfortunately, some unscrupulous brokers abuse this trust by stealing directly from their clients. These criminals may forge investor checks, transfer funds or securities without authorization, sell non-existent securities, accept undisclosed kickbacks on the sale of investments or produce false and misleading statements in the sale of the investments.

The FBI works closely with various governmental and private entities to investigate and prevent fraudulent activity in the securities markets. In an effort to help bolster these relationships and optimize workforce needs, many FBI Field Offices operate task forces and working groups with other law enforcement and regulatory agencies. These agencies include the SEC, U.S. Attorney's Office (USAO), Commodities Futures Trading Commission (CFTC) National Association of Securities Dealers (NASD), U.S. Postal Inspection Service (USPIS), and the Internal Revenue Service (IRS). Cooperation among agencies helps the FBI address the problem of Securities and Commodities Fraud more effectively and allows the FBI to more efficiently allocate its resources.

Late Day Trading: Late Day Trading is the illegal buying and selling of mutual funds after regular market hours. After the market closes each day, no one is allowed to trade mutual funds and therefore, the price remains constant. If any material information affecting a fund becomes public after hours, an opportunity is created for traders to capitalize on the set price. Traders illegally exploit this opportunity by buying or selling the fund at the closed price, knowing that the material information released will affect the value at the opening of the market and making significant illegal profits for their clients. Late Day Trading is like making your bet after you've seen your opponent's cards.

II. Overall Accomplishments

During FY 2006, the FBI investigated 1165 cases of Securities and Commodities fraud and recorded 302 indictments and 164 convictions. Many of these Securities Fraud cases are pending plea agreements or trials. The following notable statistical accomplishments are reflective in FY 2006 for Securities and Commodities Fraud: \$1.9 billion in Restitutions, \$20.6 million in Recoveries, \$80.7 million in Fines, and \$62.7 million in Seizures. The chart below is reflective of the number of pending cases from FY 2002 through FY 2006.

III. Significant Cases

INTERNATIONAL MANAGEMENT ASSOCIATES (ATLANTA):

In May 2006, Kirk Sean Wright, the founder and Chief Executive Officer of International Management Associates (IMA), was charged with 22 counts of mail fraud and three counts of Securities Fraud relating to his improper operation of IMA. IMA is a high-yield hedge fund managing more than

\$184 million in assets, including those of a group of current and former NFL players. The FBI investigation began when it learned that the athletes had been requesting disbursements from their investment accounts for several months without receiving any money. It is alleged that

Wright had misappropriated the assets of these and other IMA investors. The loss associated with this fraud is estimated to be more than \$150 million. In June 2006, Wright was arrested by the FBI on charges relating to this case. As of December 1, 2006, no trial date has been set. This case was a joint effort by the FBI, SEC, DOJ, and IRS.

BRITISH PETROLEUM; (CHICAGO):

In February 2004, British Petroleum (BP) began a scheme to manipulate the propane markets by purchasing propane and then conducting a "short squeeze." The short squeeze was an attempt to pressure "short" sellers of propane to purchase propane to cover their positions. In June 2006, a BP commodities trader pled guilty to one count of conspiracy to manipulate the price of a commodity and admitted to conspiring with others to manipulate the price of propane during February 2004. This investigation has been conducted jointly by the FBI, the Commodities Futures Trading Commission, DOJ, U.S. Attorney's Office and the U.S. Postal Inspection Service. As of December 1, 2006, a sentencing date has not been set.

U.S. Department of Justice
Federal Bureau of Investigation

FINANCIAL CRIMES SECTION
CRIMINAL INVESTIGATIVE DIVISION

HEALTH CARE FRAUD

I. General Overview

The FBI's mission in the area of Health Care Fraud is to oversee the FBI's Health Care Fraud initiatives by providing national guidance and assistance to support Health Care Fraud investigations targeting individuals and organizations who are defrauding the public and private health care systems. The FBI, along with its federal, state, and local law enforcement partners, the Centers for Medicare and Medicaid Services (CMS), and other government and privately-sponsored program participants, work closely together to address vulnerabilities, fraud, and abuse.

All health care programs are subject to fraud, however, Medicare and Medicaid programs are the most visible. Estimates of fraudulent billings to health care programs, both public and private, are estimated between 3 and 10 percent of total health care expenditures. The fraud schemes are not specific to any area, but are found throughout the entire country. The schemes target large health care programs, public and private, as well as beneficiaries. Certain schemes tend to be worked more often in certain geographical areas, and certain ethnic or national groups tend to also employ the same fraud schemes. The fraud schemes have, over time, become more sophisticated and complex, and are now being perpetrated by more organized crime groups.

Health Care Fraud is expected to continue to rise as people live longer. This increase will produce a greater demand for Medicare benefits. As a result, it is expected that the utilization of long and short term care facilities such as skilled nursing, assisted living, and hospice services will expand substantially in the future. Additionally, fraudulent billings and medically unnecessary services billed to health care insurers are prevalent throughout the country. These activities are becoming increasingly complex and can be perpetrated by corporate-driven schemes and systematic abuse by providers.

The most recent CMS statistical estimates project the total health care expenditures for FY 2006 will total \$2.16 trillion, representing 16.5 percent of the Gross Domestic Product. By the year 2012, CMS estimates total health care spending to exceed \$3.3 trillion.

With health care expenditures rising at over twice the rate of inflation, it is especially important to coordinate all investigative efforts to combat fraud within the health care system. The FBI is the primary investigative agency in the fight against Health Care Fraud, and has jurisdiction over both the federal and private insurance programs. With more than \$1 trillion being spent in the private sector on health care and its related services, the FBI's efforts are crucial to the success of the overall program. The FBI leverages its resources in both the private and public arenas through investigative partnerships with agencies such as the U.S. Department of Health and Human Services-Office of Inspector General (HHS-OIG), the Food and Drug Administration (FDA), Drug Enforcement Agency (DEA), Defense Criminal Investigative Service, Office of Personnel Management, Internal Revenue Service (IRS), and various state and local agencies. On the private

side, the FBI is actively involved with national groups, such as the National Health Care Anti-Fraud Association (NHCAA), the National Insurance Crime Bureau (NICB), the Blue Cross and Blue Shield Association (BCBSA), the American Association of Retired Persons, and the Coalition Against Insurance Fraud, as well as many other professional and grass-roots efforts to expose and investigate fraud within the system.

In furtherance of the FBI's efforts to combat Health Care Fraud in the U.S., the FBI participates in various initiatives with federal, state, and local agencies. At the Headquarters level, the FBI participates in a Senior Level Working Group which includes the CMS, DOJ, HHS-OIG, and other agencies to identify and assess health care industry vulnerabilities and make recommendations to protect the industry and the public through a coordinated effort. At the Headquarters level, the FBI is also involved in bi-weekly coordination meetings at the DOJ which includes various DOJ components involved in the fight against Health Care Fraud. National level liaison is also maintained with the DEA, FDA, Bureau of Immigration and Customs Enforcement, BCBSA, and other partners.

Throughout the country, FBI field offices participate in Health Care Fraud Working Groups which involve law enforcement agencies, prosecutors, regulatory agencies and health insurance industry professionals to identify the various crime problems involving Health Care Fraud. The FBI develops national and local initiatives when large scale fraud is detected, which may involve participation by several FBI field offices and other law enforcement agencies.

Over the years, FBI national initiatives have addressed frauds involving medical transportation, durable medical equipment, hospital cost reporting, outpatient surgery centers, pharmaceutical fraud, and a variety of other specialized investigations. FBI offices also establish state and local initiatives to meet the needs of the community. Throughout the country, various field offices have conducted their own initiatives targeting clinic, pharmacy, medical equipment, home health agency, cosmetic surgery center, and other frauds which are of great concern within a community. The FBI participates in task forces whenever possible to address specific crime problems or groups of individuals. In order to meet the needs of the private insurance industry, the FBI works very closely with the NHCAA to identify crime trends and provide training to industry and law enforcement agency personnel. Most of the insurance companies utilize an internal Special Investigations Unit and work closely with the FBI and our law enforcement partners.

Health Care Fraud investigations are among the highest priority investigations within the FBI's White Collar Crime Program, ranking behind only Public Corruption and Corporate Fraud. National initiatives include the Internet Pharmacy Fraud Initiative, the Auto Accident Insurance Fraud Initiative, and the Outpatient Surgery Center Initiative. Furthermore, numerous FBI field offices throughout the U.S. have proactively addressed significant crime problems through coordinated initiatives, task forces, and undercover operations to identify and pursue investigations against the most egregious offenders which may include organized criminal activity and criminal enterprises. Organized criminal activity has been identified in the operation of medical clinics, independent diagnostic testing facilities, durable medical equipment companies and other health care facilities. The FBI is committed to addressing this criminal activity through disruption, dismantlement, and prosecution of criminal organizations. One of the most significant trends observed in recent Health Care Fraud cases includes the willingness of medical professionals to risk patient harm in their schemes. FBI investigations in several offices are focusing on subjects who conduct unnecessary surgeries, prescribe dangerous

drugs without medical necessity, and engage in abusive or sub-standard care practices. Recent trends also suggest that advances in technology and electronic medical data have caused Health Care Fraud schemes to evolve. The FBI has developed a significant amount of expertise in investigating technical schemes involving medical data theft and other fraud schemes facilitated through the use of computers. Of course, fraud schemes continue to consist of traditional schemes that involve fraudulent billing such as billing for services not rendered and upcoding of charges for services provided

Cases initiated within the scope of the Internet Pharmacy Fraud Initiative focus on Internet websites and individuals selling illegal prescription drugs and controlled substances. The overall goal of the Internet Pharmacy Fraud Initiative is to identify fraudulent Internet pharmacies and target physicians who are willing to write prescriptions for financial gain outside of the doctor/patient relationship and with no legitimate medical purpose. Also in the scope of this initiative are investigations involving the sale of counterfeit and diverted pharmaceuticals on the Internet

The Auto Accident Insurance Fraud Initiative was launched in 2005 to address fraud schemes including organized staged accident rings and related fraudulent claims schemes. Further, the initiative targets a trend of increasingly aggressive participants in staged accident schemes who present a growing danger to others on the road. This crime problem is a threat to innocent drivers, the financial stability of the insurance industry, and the cost of auto insurance the public. Utilizing undercover investigations and other sophisticated techniques, the FBI has enhanced its commitment to addressing organized auto accident insurance fraud and continues to work closely with our NICB and private insurance partners to address this growing crime problem.

The Medicare Prescription Drug Program (Part D), implemented on January 1, 2006, has become an increasing focus and concern for the FBI. Prior to the implementation date, FBI Headquarters personnel regularly met with representatives from CMS and DOJ to share information and review fraud and abuse occurring during the enrollment period. After the implementation date, the FBI established a working group for Part D which includes representatives from CMS, DOJ, HHS-OIG, FDA, DEA, U.S. Postal Inspection Services (USPIS), and the Federal Trade Commission. This working group shares and discusses information which can be used by each agency in future investigations of fraud related to this program. The FBI has worked with CMS to obtain regional training for field office personnel of the various agencies represented in this working group. The FBI is also working through CMS to maintain dialogue with the Medicare Drug Integrity Contractors (MEDICs) who have been tasked by CMS to identify, review, and analyze cases of suspected fraud and abuse in the Part D Program.

During the past year, the FBI continued to identify and analyze industry fraud trends through input from private and public health care program experts. Present areas of concern include durable medical equipment, hospital fraud, physician fraud, home health agencies, beneficiary-sharing, chiropractic, pain management and associated drug diversion, physical therapists, prescription drugs, multi-disciplinary fraud, and identity theft which involve physician identifiers used to fraudulently bill government and private insurance programs.

As part of our national strategy to address Health Care Fraud, the FBI cooperates with the DOJ and the various U.S. Attorney's Offices throughout the country to pursue offenders through parallel criminal and civil remedies. These cases typically target large scale medical providers, such as

hospitals and corporations, who engage in criminal activity and commit fraud against the Government which undermines the credibility of the health care system. As a result, a great deal of emphasis is placed on recovering the illegal proceeds through seizure and forfeiture proceedings as well as substantial civil settlements. Upon the successful conviction of Health Care Fraud offenders, the FBI provides assistance to various regulatory and state agencies which may seek exclusion of convicted medical providers from further participation in the Medicare and Medicaid health care systems.

The FBI and the health care industry continue to expand their technology and intelligence assessments through the use of sophisticated data mining techniques to identify patterns of fraud, systemic weaknesses, and aberrant billing activity.

II. Overall Accomplishments

Through FY 2006, 2,423 cases investigated by the FBI resulted in 588 indictments and 534 convictions of Health Care Fraud criminals. Numerous cases are pending plea agreements and trials. The following notable statistical accomplishments are reflective in FY 2006 for Health Care Fraud: \$373 million in Restitutions, \$1.6 billion in Recoveries, \$172.9 million in Fines, and \$24.3 million in Seizures. The chart below is reflective of the number of pending cases from FY 2002 through FY 2006.

III. Significant Cases

JORGE A. MARTINEZ, M.D. (CLEVELAND):

This investigation resulted in the first known prosecution involving a criminal charge of Health Care Fraud resulting in death. The case focused on the illegal distribution of pharmaceutical narcotics and billing for unnecessary medical procedures. The investigation revealed that Dr. Martinez provided excessive narcotic prescriptions, including OxyContin, to patients in exchange for the patients enduring unnecessary nerve block injections. Dr. Martinez' actions directly resulted in the death of two of his patients. From 1998 until his arrest in 2004, Martinez submitted more than \$59 million in claims to Medicare, Medicaid, and the Ohio Bureau of Worker's Compensation. In January 2006, a jury found Martinez guilty of 56 criminal counts, including distribution of controlled substances, mail fraud, wire fraud, Health Care Fraud, and Health Care Fraud resulting in death. Martinez was later sentenced to life in prison. This investigation was conducted jointly with the HHS-OIG, Ohio Bureau of Workers Compensation, DEA Diversion, AdvanceMed, Ohio Department of Job and Family Services, Anthem Blue Cross Blue Shield and Medical Mutual of Ohio.

BANSAL ORGANIZATION (PHILADELPHIA):

This investigation was conducted jointly with the DEA and IRS and was focused on a Philadelphia-based Internet pharmacy drug distributor which was smuggling drugs into the U.S. from India and selling them over the Internet. The criminal organization shipped several thousand packages per week to individuals around the country. In April 2005, 24 individuals were indicted on charges of distributing controlled substances, importing controlled substances, involvement in a continuing criminal enterprise, introducing misbranded drugs into interstate commerce, and participating in money laundering. Over \$8 million has been seized to date as a result of the charges. As of December 1, 2006, 12 suspects have plead guilty, three have been convicted at trial, four are in foreign custody, and five remain fugitives. This investigation was worked jointly with the DEA, IRS, ICE, USPIIS, and the Lower Merion Police Department.

Health Care Fraud is carried out by many segments of the health care system using various methods. Some of the most prevalent schemes include:

Billing for Services not Rendered – These schemes can have several meanings and could include any of the following:

- No medical service of any kind was rendered.
- The service was not rendered as described in the claim for payment.
- The service was previously billed and the claim had been paid.

Upcoding of Services – This type of scheme involves a billing practice where the health care provider submits a bill using a procedure code that yields a higher payment than the code for the service that was truly rendered. The upcoding of services varies according to the provider type. Examples of service upcoding include:

- A routine, follow-up doctor's office visit being billed as an initial or comprehensive office visit.
- Group therapy being billed as individual therapy.
- Unilateral procedures being billed as bilateral procedures.
- 30-minute sessions being billed as 50+ minute sessions.

Upcoding of Items – A medical supplier is upcoding when, for example, the supplier delivers to the patient a basic, manually propelled wheelchair, but bills the patient's health insurance plan for a more expensive motorized version of the wheelchair.

Duplicate Claims – A duplicate claim usually involves a certain item or service for which two claims are filed. In this scheme, an exact copy of the claim is not filed a second time; rather, the provider usually changes a portion (most often the date of service) of the claim so that the health insurer will not realize that the claim is a duplicate. In other words, the exact claim is not filed twice, but one service is billed two times in an attempt to be paid twice for one service.

Unbundling – This is the practice of submitting bills in a fragmented fashion in order to maximize the reimbursement for various tests or procedures that are required to be billed together at a reduced cost. For example, clinical laboratory tests may be ordered individually or in a “panel” (i.e. a lipid panel, an arthritis panel, a hepatitis panel). Billing tests within each panel as though they were done individually on subsequent days is an example of unbundling.

Excessive Services – These schemes typically involve the provision of medical services or items which are in excess of the patient’s actual needs. Examples of excessive services include:

- A medical supply company delivering and billing for 30 wound care kits per week for a nursing home patient who only requires a change of dressings once per day.
- Daily medical office visits conducted and billed for when monthly office visits would be more than adequate.

Medically Unnecessary Services – A service is medically unnecessary and may give rise to a fraudulent scheme when the service is not justified by the patient's medical condition or diagnosis. For example, a claim for payment for an electrocardiogram (EKG) test may be fraudulent if the patient has no conditions, complaints, or factors which would necessitate the test.

Kickbacks – A health care provider or other person engages in an illegal kickback scheme when he or she offers, solicits, pays or accepts money or something of value in exchange for the referral of a patient for health care services that may be paid for by Medicare or Medicaid. A laboratory owner and doctor each violate the Anti-Kickback statute when the laboratory owner pays the doctor \$50 for each Medicare patient the doctor sends to the laboratory for testing. Although kickbacks are often paid in cash based on a percentage of the amount paid by Medicare or Medicaid for a service, kickbacks may take other forms such as jewelry, free paid vacations, or other valuable items.

HEALTH CARE FRAUD PREVENTION MEASURES

Health Care Fraud is not a victimless crime. It increases healthcare costs for everyone. It is as dangerous as identity theft. Fraud has left many thousands of people injured. Participation in Health Care Fraud is a crime.

Keeping America's health system free from fraud requires active participation from each of us. The large number of patients, treatments and complex billing practices attract criminals skilled in victimizing innocent people by committing fraud.

What is Health Care Fraud?

- Altered or fabricated medical bills and other documents.
- Excessive or unnecessary treatments.
- Billing schemes, such as:
 - charging for a service more expensive than the one provided.
 - charging for services that were not provided.
 - duplicate charges.
- False or exaggerated medical disability.
- Collecting on multiple policies for the same illness or injury.

Tips to protect yourself against Health Care Fraud

- Protect your health insurance information card like a credit card.
- Beware of free services--is it too good to be true?
- Review your medical bills after receiving healthcare services--Check that the dates and services are correct to ensure you get what you paid for.
- If you suspect Health Care Fraud, call 1-877-327-2583. For more information, visit the web site at <http://www.bcbs.com/antifraud>.

U. S. Department of Justice
Federal Bureau of Investigation

FINANCIAL CRIMES SECTION
CRIMINAL INVESTIGATIVE DIVISION

MORTGAGE FRAUD

I. General Overview

The increased reliance by both financial institutions and non-financial institution lenders on third-party brokers has created opportunities for organized fraud groups, particularly where mortgage industry professionals are involved.

Combating significant fraud in this area is a priority, because mortgage lending and the housing market have a significant overall effect on the nation's economy. All Mortgage Fraud programs were recently consolidated within the Financial Institution Fraud Unit, even where the targeted lender is not a financial institution. This consolidation provides a more effective and efficient management over Mortgage Fraud investigations, the ability to identify and respond more rapidly to emerging Mortgage Fraud problems and a clearer picture of the overall Mortgage Fraud problem.

Each Mortgage Fraud scheme contains some type of "material misstatement, misrepresentation, or omission relating to the property or potential mortgage relied on by an underwriter or lender to fund, purchase or insure a loan." The Mortgage Bankers Association projects \$2.37 trillion in mortgage loans will be made during 2006. The FBI compiles data on Mortgage Fraud through Suspicious Activity Reports (SARs) filed by federally-insured financial institutions and Department of Housing and Urban Development Office of Inspector General (HUD-OIG) reports. The FBI also receives complaints from the mortgage industry at large.

A significant portion of the mortgage industry is void of any mandatory fraud reporting. In addition, as initial mortgage products are repackaged and sold on secondary markets, the sale of the mortgages, in many cases conceal or distort the fraud, causing it not to be reported. Therefore, the true level of Mortgage Fraud is largely unknown. The mortgage industry itself does not provide estimates on total industry fraud. However, based on various industry reports and FBI analysis, Mortgage Fraud is pervasive and growing.

The FBI investigates Mortgage Fraud in two distinct areas: Fraud for Profit and Fraud for Housing. Fraud for Profit is sometimes referred to as "Industry Insider Fraud" and the motive is to revolve equity, falsely inflate the value of the property, or issue loans based on fictitious properties. Based on existing investigations and Mortgage Fraud reporting, 80 percent of all reported fraud losses involve collaboration or collusion by industry insiders. Fraud for Housing represents illegal actions perpetrated solely by the borrower. The simple motive behind

this fraud is to acquire and maintain ownership of a house under false pretenses. This type of fraud is typified by a borrower who makes misrepresentations regarding his income or employment history to qualify for a loan.

The defrauding of mortgage lenders should not be compared to predatory lending practices which primarily affect borrowers. Predatory lending typically effects senior citizens, lower income and challenged credit borrowers. Predatory lending forces borrowers to pay exorbitant loan origination/settlement fees, sub-prime or higher interest rates and in some cases, unreasonable service fees. These practices often result in the borrower defaulting on his mortgage payment and undergoing foreclosure or forced refinancing.

Although there are many Mortgage Fraud schemes, the FBI is focusing its efforts on those perpetrated by industry insiders. The FBI is engaged with the mortgage industry primarily in identifying fraud trends and educating the public. Some of the current rising Mortgage Fraud trends include: equity skimming, property flipping, and mortgage related identity theft. Equity skimming is a tried and true method of committing Mortgage Fraud. Today's common equity skimming schemes involve the use of corporate shell companies, corporate identity theft, and the use or threat of bankruptcy/foreclosure to dupe homeowners and investors. Property flipping is nothing new; however, once again law enforcement is faced with an educated criminal element that is using identity theft, straw borrowers and shell companies, along with industry insiders to conceal their methods and override lender controls.

Property flipping is best described as purchasing properties and artificially inflating their value through false appraisals. The artificially valued properties are then repurchased several times for a higher price by associates of the "flipper." After three or four sham sales, the properties are foreclosed on by victim lenders. Often flipped properties are ultimately repurchased for 50 to 100 percent of their original value.

Since 1999, the FBI has been actively investigating Mortgage Fraud in various cities across the U.S. The FBI also focuses on fostering relationships and partnerships with the mortgage industry to promote Mortgage Fraud awareness. To raise awareness of this issue and provide easy accessibility to investigative personnel, the FBI has provided points-of-contact to relevant groups including the Mortgage Bankers Association (MBA), the Mortgage Asset Research Institute, the Mortgage Insurance Companies of America, Fannie Mae, Freddie Mac, and others.

The FBI has also been working to establish broader SAR reporting requirements for mortgage lenders who do not have adequate protection under the current safe harbor provisions. The FBI is collaborating with the mortgage industry and Financial Crimes Enforcement Network (FinCEN) to create a more productive reporting requirement for Mortgage Fraud. The FBI has also been working with the FinCEN to promote an efficient and effective method of identifying and reporting fraudulent mortgage activity affecting non-federally insured mortgage institutions.

The FBI works closely with individual lenders, as well as national associations such as the MBA, the Appraisal Institute, the National Association of Mortgage Brokers, and the National Notary Association, to define and combat the Mortgage Fraud problem. In addition, on

a case-by-case basis, the FBI receives close cooperation from lenders. An example of this is the usage of Real Estate Owned properties from lender inventories to facilitate Mortgage Fraud undercover operations (UCO). In December 2003, the FBI initiated an UCO to address the massive amount of Mortgage Fraud in the Jacksonville area. On September 16, 2004, as a result of this investigation, seven search warrants were executed and two arrests were made. Mortgage broker J.R. Parker and closing attorney Dale Beardsley, were arrested, charging them with bank

fraud for their role in this scheme. On or about October 2005, Parker and Beardsley were convicted of conspiracy, mail fraud, and wire fraud. In addition, seizures in the case included two homes valued at over \$1million each, six luxury cars and a money judgment in the amount of \$14 million. This UCO was made possible by the close cooperation of a local financial institution. This type of cooperation happens around the country and is a key component in the FBI's approach to this growing crime problem.

Regional analysis of suspicious activity reports (SARS) indicating Mortgage Fraud violations indicates the West region of the U.S. led the nation with 35.9 percent of Mortgage Fraud-related SARs filed during FY 2006. The Central, Southeast, and Northeast regions had 24.7, 22.6 and 16.9 percent respectively of Mortgage Fraud related SAR filings. However, FBI pending cases indicated that the Central region had the majority of Mortgage Fraud cases with 33.3 percent during 2006. The West, Southeast, and Northeast had 26.7, 27.2 and 12.8 percentages respectively. FBI pending cases by region are consistent with Mortgage Asset Research Institute (MARI) reporting which indicated that five of the top ten Mortgage Fraud affected states in 2006 were located in the Central region.

Mapping data from FY 2005 SARs, FBI pending Mortgage Fraud cases, Federal Housing Authority (FHA)-insured loans defaulting between October 1, 2003 and September 30, 2001 and 2005 MARI data, reveals the top 16 states for Mortgage Fraud activity. States documented by three or four sources include California, Colorado, Florida, Georgia, Illinois, Michigan, and Texas. States documented by two sources include North Carolina, Ohio, Utah, and Missouri, and states documented by one source include: Arizona, Indiana, Louisiana, New York, and South Carolina. (See map below).

II. Overall Accomplishments

Through FY 2006, 818 cases investigated by the FBI resulted in 263 indictments and 204 convictions of Mortgage Fraud criminals. The following notable statistical accomplishments are reflective in FY 2006 for Mortgage Fraud: \$388.9 million in Restitutions, \$1.4 million in Recoveries, and \$231 million in Fines. The chart below is reflective of the number of pending cases from FY 2003 through FY 2006.

III. Significant Cases

AMERIFUNDING (DENVER):

Amerifunding was a Mortgage Brokerage owned and operated by Gerald Small in Colorado, which maintained two "warehouse" lines of credits, each at a large federally-insured financial institution in the U.S. In order to support a lavish lifestyle, Small created fictitious loans to live off of the lines of credit. The borrower information, name, and social security number, were invented. Eventually, one of the creditors asked for verification of identification thereby defeating the "invention" process. To deal with this, Small placed an advertisement for a \$100,000+ Account Representative position at his company. Applicants eagerly completed applications inclusive of names, social security numbers and copies of driver's licenses which Small wasted no time in utilizing for more fictitious loans. Investigation determined that Small had kited over \$200 million in fraudulent mortgage loans and used the stolen identities of 47 job applicants to obtain mortgage funding for fictitious home loans, or "air loans" totaling over \$21.5 million during a 24-month period.

Gerald Small engaged with others in a massive Kiting and Mortgage Fraud scheme in Colorado resulting in the conviction of six individuals, the seizure of almost \$20 million in cash and assets, the restitution of two private jet aircraft, and losses to federally- insured financial institutions of approximately \$35 million.

MIDTOWNE RESTORATION LLC (KANSAS CITY):

Brent Michael Barber led the Mortgage Fraud ring holding himself and company Midtowne Restoration LLC as a real estate investment company. "Straw Buyers" were solicited in schemes where they were paid \$2,000 for use of their identity and credit profiles to obtain mortgage financing for properties predominately in low income areas of Kansas City, Missouri. In other schemes, investors were recruited for properties which were represented to be refurbished and appraised at amounts far in excess of their true value. The investors were assured by Barber that renters would be found to service the mortgage and maintenance costs of the properties so there would be no risk.

On February 23, 2006, Barber pled guilty to 104 counts contained in two federal indictments, and was convicted by a jury for a fraud covered by a third federal indictment.

Also convicted in the schemes were eight individuals which involved about 300 fraudulent mortgage loans worth approximately \$19.6 million and caused losses to federally-insured financial institutions of approximately \$11.8 million. On October 27, 2006, Barber was sentenced to 12 years and 7 months federal incarceration, and ordered to pay restitution in the amount of \$11,206,419.

MORTGAGE FRAUD INDICATORS

- Inflated Appraisals
- Exclusive use of one appraiser
- Increased Commissions/Bonuses - Brokers and Appraisers
- Bonuses paid (outside or at settlement) for fee-based services
- Higher than customary fees
- Falsifications on Loan Applications
- Buyers told/explained how to falsify the mortgage application
- Requested to sign blank application
- Fake Supporting Loan Documentation
- Requested to sign blank employee or bank forms
- Requested to sign other types of blank forms

- Purchase Loans Disguised as Refinance
- Purchase loans that are disguised as refinances
 - requires less documentation/lender scrutiny

- Investors-Short Term Investments with Guaranteed Re-Purchase
- Investors used to flip property prices for fixed percentage
- Multiple "Holding Companies" utilized to increase property values

COMMON MORTGAGE FRAUD SCHEMES

Property Flipping - Property is purchased, falsely appraised at a higher value, and then quickly sold. What makes property illegal is that the appraisal information is fraudulent. The schemes typically involve one or more of the following: fraudulent appraisals, doctored loan documentation, inflating buyer income, etc. Kickbacks to buyers, investors, property/loan brokers, appraisers, and title company employees are common in this scheme. A home worth \$20,000 may be appraised for \$80,000 or higher in this type of scheme.

Silent Second - The buyer of a property borrows the down payment from the seller through the issuance of a non-disclosed second mortgage. The primary lender believes the borrower has invested his own money in the down payment, when in fact, it is borrowed. The second mortgage may not be recorded to further conceal its status from the primary lender.

Nominee Loans/Straw Buyers - The identity of the borrower is concealed through the use of a nominee who allows the borrower to use the nominee's name and credit history to apply for a loan.

Fictitious/Stolen Identity - A fictitious/stolen identity may be used on the loan application. The applicant may be involved in an identity theft scheme: the applicant's name, personal identifying information, and credit history are used without the true person's knowledge.

Inflated Appraisals - An appraiser acts in collusion with a borrower and provides a misleading appraisal report to the lender. The report inaccurately states an inflated property value.

Foreclosure Schemes - The perpetrator identifies homeowners who are at risk of defaulting on

loans or whose houses are already in foreclosure. Perpetrators mislead the homeowners into believing that they can save their homes in exchange for a transfer of the deed and up-front fees. The perpetrator profits from these schemes by remortgaging the property or pocketing fees paid by the homeowner.

Equity Skimming - An investor may use a straw buyer, false income documents, and false credit reports, to obtain a mortgage loan in the straw buyer's name. Subsequent to closing, the straw buyer signs the property over to the investor in a quit claim deed which relinquishes all rights to the property and provides no guaranty to title. The investor does not make any mortgage payments and rents the property until foreclosure takes place several months later.

Air Loans - This is a non-existent property loan where there is usually no collateral. An example of an air loan would be where a broker invents borrowers and properties, establishes accounts for payments, and maintains custodial accounts for escrows. They may set up an office with a bank of telephones, each one used as the employer, appraiser, credit agency, etc., for verification purposes.

Mortgage Fraud Prevention Measures

General Fraud Tips

Mortgage Fraud is a growing problem throughout the U.S. People want to believe their homes are worth more than they are, and with housing booms going on throughout the U.S., there are people who try to capitalize on the situation and make an easy profit.

Tips to protect you from becoming a victim of Mortgage Fraud

Get referrals for real estate and mortgage professionals. Check the licenses of the industry professionals with state, county, or city regulatory agencies.

- If it sounds too good to be true, it *probably* is. An outrageous promise of extraordinary profit in a short period of time signals a problem.
- Be wary of strangers and unsolicited contacts, as well as high-pressure sales techniques.
- Look at written information to include recent comparable sales in the area, and other documents such as tax assessments to verify the value of the property.
- Understand what you are signing and agreeing to--If you do not understand,
 - re-read the documents, or seek assistance from an attorney.
- Make sure the name on your application matches the name on your identification.
- Review the title history to determine if the property has been sold multiple times within a short period--It could mean that this property has been "flipped" and the value falsely inflated.
- Know and understand the terms of your mortgage--Check your information against the information in the loan documents to ensure they are accurate and complete.
- Never sign any loan documents that contain blanks--This leaves you vulnerable to fraud.
- Check out the tips on the Mortgage Bankers Association's (MBA) website at <http://www.StopMortgageFraud.com> for additional advice on avoiding Mortgage Fraud.

- Mortgage Debt Elimination Schemes
- Be aware of e-mails or web-based advertisements that promote the elimination of mortgage loans, credit card, and other debts while requesting an up-front fee to prepare documents to satisfy the debt. The documents are typically entitled Declaration of Voidance, Bond for Discharge of Debt, Bill of Exchange, Due Bill, Redemption Certificate, or other similar variations. These documents do not achieve what they purport.
- There is no magic cure-all to relieve you of debts you incurred.
- Borrowers may end up paying thousands of dollars in fees without the elimination or reduction of any debt.

Foreclosure Fraud Schemes

Perpetrators mislead the homeowners into believing that they can save their homes in exchange for a transfer of the deed, usually in the form of a Quit-Claim Deed, and up-front fees. The perpetrator profits from these schemes by re-mortgaging the property or pocketing fees paid by the homeowner without preventing the foreclosure. The victim suffers the loss of the property as well as the up-front fees.

- Be aware of offers to "save" homeowners who are at risk of defaulting on loans or whose houses are already in foreclosure.
- Seek a qualified Credit Counselor or attorney to assist.

Predatory Lending Schemes

- Before purchasing a home, research information about prices of homes in the neighborhood.
- Shop for a lender and compare costs. Beware of lenders who tell you that they are your only chance of getting a loan or owning your own home.
- Beware of "No Money Down" loans--This is a gimmick used to entice consumers to purchase property that they likely cannot afford or are not qualified to purchase. Be wary of mortgage professional who falsely alter information to qualify the consumer for the loan.
- Do not let anyone convince you to borrow more money than you can afford to repay.
- Do not let anyone persuade you into making a false statement such as overstating your income, the source of your down payment, or the nature and length of your employment.
- Never sign a blank document or a document containing blanks.
- Read and carefully review all loan documents signed at closing or prior to closing for accuracy, completeness, and omissions.
- Be aware of cost or loan terms at closing that are not what you agreed to.
- Do not sign anything you do not understand.
- Be suspicious if the cost of a home improvement goes up if you accept the contractor's financing.
- If it sounds too good to be true--it *probably* is!

IDENTITY THEFT

I. General Overview

Identity theft involves the misuse of another individual's personal identifying information for fraudulent purposes. It is almost always committed to facilitate other crimes, such as credit card fraud, mortgage fraud, and check fraud. Personal identifying information, such as name, Social Security number, date of birth and bank account number is extremely valuable to an identity thief. With relatively little effort, an identity thief can use this information to take over existing credit accounts, create new accounts in the victim's name or even evade law enforcement after the commission of a violent crime. Identity thieves also sell personal information online to the highest bidder, often resulting in the stolen information being used by a number of different perpetrators. Identity theft can be very difficult for consumers to deal with, as they often do not know they have been defrauded until they are denied credit or receive a call from a creditor seeking payment for a debt incurred in their name.

Although not a new crime, identity theft has evolved into a serious and pervasive threat to consumers and the financial services industry alike. Estimates vary on the true impact of the problem, but law enforcement and consumer advocacy groups agree that financial institutions lose billions of dollars each year to identity theft and consumers face additional hardships, ranging from financial loss to time spent trying to undo the harm caused to their credit records and other aspects of their lives. Identity theft also puts significant demands on law enforcement, as federal, state, and local law enforcement agencies and prosecutors grapple with venue issues and limited resources, which can complicate their efforts to effectively deal with the problem.

A survey conducted by the Federal Trade Commission (FTC) in 2006 estimated that 8.3 million American consumers, or 3.7 percent of the adult population, became victims of identity theft in 2005. Most of the financial losses are suffered by credit issuers and banks, as victims are rarely held responsible for fraudulent debts incurred in their name; however, victims often bear the responsibility of contacting their banks and credit issuers after an identity theft has occurred. The same FTC survey determined that victim consumers spent over 200 million hours in 2005 attempting to recover from identity theft.

Law enforcement agencies across the country have formed task forces and working groups to address the identity theft problem. The FBI currently participates in 21 task forces and working groups dedicated to identity theft and over 80 other financial crimes task forces. In cities such as Detroit, Chicago, Los Angeles, and Salt Lake City, identity fraud task forces are realizing significant success. For example, in FY 2005 the Detroit Metropolitan Identity Fraud Task Force accumulated the following statistical accomplishments: 23 search warrants, 23 arrest warrants, 37 arrests, 11 indictments, 29 convictions, 69 fraud cells identified, and 23 identity fraud organizations dismantled. In addition, the FBI has dedicated significant analytical resources to

combating the identity theft problem and is working with the President's Identity Theft Task Force and other agencies such as the FTC to develop a system that will analyze large streams of identity theft data and refer the results to law enforcement agencies in order to proactively target organized groups of identity thieves.

Although the total number of FBI identity theft-related cases has decreased from 1,678 in FY 2005 to 1,255 in FY 2006, our field offices have been aggressively pursuing identity theft charges in many of our investigations, ranging from traditional bank fraud cases to counterterrorism cases. To effectively utilize our resources, investigations typically focus on organized groups of identity thieves and criminal enterprises which are the most difficult to investigate and often involve a substantial number of victims. The FBI and other government agencies have initiated consumer education programs which have made consumers more aware of the perils of leaving personal information unprotected. The financial services industry is also doing its part to make its financial products less susceptible to fraud.

II. Overall Accomplishments

Through FY 2006, 1255 cases investigated by the FBI resulted in 457 indictments and 405 convictions of Identity Theft criminals. The following notable statistical accomplishments are reflective in FY 2006 for Identity Theft Fraud across all FBI Programs: \$156.5 million in Restitutions, \$4.3 million in Recoveries, and \$1.2 million in Fines. The chart below is reflective of the number of pending cases from FY 2003 through FY 2006.

III. Significant Cases

OLATUNJI OLUWATOSIN (LOS ANGELES):

On February 10, 2006, Olatunji Oluwatosin, a Nigerian national residing in North Hollywood, California was sentenced to 10 years in prison and ordered to pay restitution of \$6.5 million for his role in a scheme that potentially compromised the identities of over 165,000 people nationwide. Oluwatosin, doing business as Pacific Collections, gained access to a consumer database and obtained personal information on numerous consumers. He then used the information to establish at least 10 fraudulent business accounts, which allowed him and his associates to access the personal information of numerous consumers. Some of the information was used to take over existing credit card accounts or establish new accounts in the victims' names. This case was investigated by the Southern California High Tech Task Force Identity Theft Detail, including the FBI and the Los Angeles County Sheriff's Department.

HAROLD MCCOY; ET AL (PHILADELPHIA):

On June 16, 2006, Harold McCoy was sentenced to 162 months in prison following a guilty plea to charges of bank fraud, identity theft, and conspiracy for his role in a scheme to defraud numerous American Red Cross (ARC) blood donors in the Philadelphia area. McCoy obtained the names and personal identifying information of numerous blood donors from an employee of ARC. He and his co-conspirators, Karynn Long and Danielle Baker, then used the stolen information to obtain instant credit loans, bank loans, and to cash counterfeit checks, causing approximately \$800,000 in losses to various financial institutions. This crime jeopardized the Philadelphia area blood supply and damaged ARC's trusted relationship with the public, as many people stopped donating blood and two corporate donation centers ceased their blood drives when the media reported the crime. For their roles in this scheme, Long pled guilty to bank fraud and conspiracy and was sentenced to 18 months in prison; Baker pled guilty to identity theft and conspiracy and was sentenced to 24 months in prison. All three defendants were ordered to pay restitution in the amount of \$270,555.

Indications of Identity Theft

The following occurrences are some of the indications of identity theft:

- Charges occurring on your accounts that you did not authorize.
- If your credit is denied due to poor credit ratings, despite good credit history.
- If you are contacted by creditors regarding amounts owed for goods or services that you never obtained or authorized.
- If your credit card and bank statements are not received in the mail as expected.
- If a new or renewed credit card is not received.

Identity Theft/Fraud Prevention Measures

U.S. citizens need to be aware of measures that can be taken to either prevent or minimize their chances of becoming a victim of fraud. Some of these measures are as follows:

- Never give personal information via telephone, mail or the Internet,
- unless you initiated the contact.
- Store personal information in a safe place.
- Shred credit card receipts and/or old statements before discarding

- in a garbage can--If you do not have a shredder, then use scissors.
- Protect PINs and passwords.
- Carry only the minimum amount of identifying information.
- Remove your name from mailing lists for pre-approved credit lines and tele-marketers.
- Order and closely review biannual copies of your credit report from each national credit reporting agency (Equifax, Experian, and Trans Union).
- Request DMV to assign an alternate driver's license number if it currently features your Social Security account number.
- Ensure that your PIN numbers cannot be observed by anyone while utilizing an ATM or public telephone.
- Close all unused credit card or bank accounts.
- Contact your creditor or service provider if expected bills do not arrive.
- Check account statements carefully.
- Guard your mail from theft.
- BE AWARE!

If You are a Victim of Identity Theft

- These steps are among those that should be completed by persons who believe they have been the victim of an identity theft:
- Contact the fraud departments of the three major credit bureaus to place fraud alerts on your credit file in order to reduce your risk of further victimization.
- Obtain and review a current copy of your credit report to determine whether any unknown fraud has occurred--(You will need to more closely monitor your credit going forward as some identity thefts can continue for extended periods of time).
- Contact the account issuer(s) where fraudulent accounts have been opened or where your accounts have been taken over--Ask for the fraud/security department and notify them both via telephone and in writing.
- Close all tampered or fraudulent accounts.
- Ask about the existence of secondary cards.
- Contact your local police department and file a police report.
- Notify the police department in the community where the identity theft occurred, if it is different from your own.
- Obtain copies of any police reports filed.
- Keep a detailed log of who you talked to and when, including their title, phone number, and other contact information.
- Contact the Federal Trade Commission's Identity Theft Clearinghouse and file an identity theft complaint at www.consumer.gov/idtheft. [Those complaints are utilized by law enforcement agencies, including the FBI, that investigate identity theft. You can also obtain additional information at that website regarding your rights as a victim.](#)
- Online identity thefts can also be reported at www.IC3.gov.

U. S. Department of Justice
Federal Bureau of Investigation

FINANCIAL CRIMES SECTION
CRIMINAL INVESTIGATIVE DIVISION

INSURANCE FRAUD

I. General Overview

Insurance fraud continues to be an investigative priority for the FBI's Financial Crimes Section, due in large part to the insurance industry's significant status in the U.S. economy. The U.S. insurance industry consists of thousands of companies and collects nearly \$1 trillion in premiums each year. The size of the industry, unfortunately, makes it a prime target for criminal activity; the Coalition Against Insurance Fraud (CAIF) estimates that the cost of fraud in the industry is as high as \$80 billion each year. This cost is passed on to consumers in the form of higher premiums. In fact, the National Insurance Crime Bureau (NICB) calculates that insurance fraud raises the yearly cost of premiums by \$300 for the average household.

The FBI is attempting to identify the most prevalent schemes and the top echelon criminals defrauding the insurance industry in an effort to reduce this type of fraud. The FBI works closely with the National Association of Insurance Commissioners, NICB, CAIF, as well as state fraud bureaus, state insurance regulators, and other federal agencies to combat insurance fraud. In addition, the FBI is a member of the International Association of Insurance Fraud Agencies, an international non-profit organization whose mission is to maintain an international presence to address insurance and insurance-related financial crimes on a global basis. Currently, the FBI is focusing a majority of its resources relating to insurance fraud on the following schemes:

Hurricane Katrina Insurance Fraud - In late August 2005, Hurricane Katrina made landfall along America's Gulf Coast, severely damaging the region and causing approximately \$100 billion in damages. According to the CAIF, Katrina generated approximately 1.6 million insurance claims totaling \$34.4 billion in insured losses. The destruction caused by the storm has resulted in a marked increase in insurance fraud in the area. Of the more than 80 billion government dollars appropriated for reconstruction efforts in the region, it is estimated that insurance fraud accounts for between \$4 and \$6 billion.

Insurance fraud related to the 2005 hurricane season has taken on a variety of forms. Policy holders, for example, have been tempted to exaggerate or falsify claims in the wake of Katrina. According to the Louisiana State Police, many policy holders without flood insurance are submitting fire or stolen property claims for items that were actually damaged by flood waters. Additionally, some policyholders are "double dipping"--that is, holding multiple policies with

different carriers, claiming the same damage expenses with both companies, and eventually receiving two payments for what should have been one claim. Other individuals are intentionally damaging their own property in order to increase repair cost estimates, ultimately increasing the payments they receive from insurers.

Other fraud stemming from Hurricane Katrina is perpetrated by unscrupulous contractors. In one

common scheme, contractors are convincing victims that a deposit is required before a job can be initiated. After receiving the deposit money, however, the contractors fail to complete, or even begin, the agreed upon repair work. Another fraudulent scheme used by corrupt contractors is "bid-rigging." In bid-rigging, contractors raise the cost of a construction job by conspiring in the bidding process. The homeowner is quoted two inflated bids and one lower (but still inflated) bid. The work is completed by the lowest bidder and kickbacks are paid to the other firms and the homeowner.

Insurance-Related Corporate Fraud - Although Corporate Fraud is not unique to any particular industry, there has been a recent trend involving insurance companies caught in the web of these schemes. The temptations for fraud within the corporate industry can be greater during periods of financial downturns. Insurance companies hold customer premiums which are forbidden from operational use by the company. However, when funding is needed, unscrupulous executives invade the premium accounts in order to pay corporate expenses. This leads to financial statement fraud because the company is required to "cover its tracks" to conceal the improper utilization of customer premium funds.

Premium Diversion/Unauthorized Entities - The most common type of fraud involves insurance agents and brokers diverting policyholder premiums for their own benefit. Additionally, there is a growing number of unauthorized and unregistered entities engaged in the sale of insurance-related products. As the insurance industry becomes open to foreign players, regulation becomes more difficult. Additionally, exponentially rising insurance costs in certain areas (i.e., terrorism insurance, directors'/officers' insurance, and corporations), increases the possibility for this type of fraud. The schemes typically involve entities which utilize a myriad of sophisticated schemes for verification of submitted fraudulent financial statements to the state insurance regulatory body in order to hide the true nature of the fictitious assets listed in the statements. This generates large insurance premiums solely to be diverted.

Viatical Settlement Fraud - A viatical settlement is a discounted, pre-death sale of an existing life insurance policy on the life of a person known to have a terminal condition. The parties to a viatical settlement include the insured party, insurance agent/broker, insurance company, viatical company/broker, and the investor. Viatical settlement fraud occurs when misrepresentations are made on the insurance policy applications, in effect, hiding the fact that the party applying for a policy has already been diagnosed with a terminal condition. On the investor end, the fraud occurs when misrepresentations are made to the investors by the viatical companies about life expectancies of insured parties and guaranteed high rates of return.

With the cooperation of the insurance industry, through referrals from industry liaison and other law enforcement agencies, the FBI continues to target the individuals and organizations committing insurance fraud. The FBI continues to initiate and conduct traditional investigations as well as utilize sophisticated techniques, to include undercover investigations, to apprehend the fraudsters.

Workers Compensation Fraud - The Professional Employer Organization (PEO) industry operates chiefly to provide workers compensation insurance coverage to small businesses by pooling businesses together to obtain reasonable rates. Workers compensation insurance accounts for as much as 46 percent of a small business owners' general operating expenses. Due to this, small business owners have an incentive to shop workers compensation insurance on a regular

basis. This has made it ripe for entities who purport to provide workers compensation insurance to enter the marketplace, offer reduced premium rates and misappropriate funds without providing insurance. The focus of these investigations is on allegations that numerous entities within the PEO industry are selling unauthorized and non-admitted workers compensation coverage to businesses across the U.S. This insurance fraud scheme has left injured and deceased victims without workers compensation coverage to pay their medical bills.

II. Overall Accomplishments

III. Significant Cases

HURRICANE KATRINA RELATED FRAUD (SACRAMENTO):

In the wake of Hurricane Katrina, The American Red Cross established a national call center in Bakersfield, California to process and disburse relief funds to victims of the disaster. After the Red Cross noticed a disproportionate amount of disbursements in the immediate Bakersfield area when compared to the rest of the state, an investigation was launched. It is estimated that \$500,000 was lost due to fraud conducted by workers at the call center. As of December 1, 2006, a total of 73 individuals have been indicted in the case, including 24 Red Cross contract employees, 61 subjects who have pled guilty to various felony charges, including charges of wire fraud and false statements and 25 subjects have been sentenced. A Hurricane Katrina Fraud Task Force, consisting of FBI, DOJ, U.S. Attorneys' Offices, Office of Inspector General, U.S. Secret Service, the Federal Trade Commission, the Securities and Exchange Commission and various state and local law enforcement agencies has been initiated to address frauds relating to the Hurricane.

MUTUAL BENEFITS CORPORATION (MIAMI):

Mutual Benefits Corporation (MBC) was a viatical settlement company offering interests in insurance policies to investors worldwide. Over 28,000 investors worldwide were defrauded of approximately \$956 million by the principals of MBC, who misrepresented the investment and failed to disclose prior regulatory actions. Additionally, MBC falsified the life expectancies of the insured and paid kickbacks to physicians for signing fraudulent documents that were provided to investors. In October 2006, Peter Lombardi, former MBC President, pled guilty to Securities Fraud. As a part of his plea agreement, Lombardi has agreed to be responsible for \$956 million in restitution to the victim investors in this fraud. The SEC and IRS assisted in this investigation.

MASS MARKETING FRAUD

I. General Overview

Mass Marketing Fraud is a general term for frauds that exploit mass-communication media, such as telemarketing fraud, Internet fraud, and identity theft. Since the 1930's, mass marketing has been an accepted and productive way of increasing a customer base. Advanced communications, including computers, speed dialing, automatic dialing, and facsimile machines, along with modern conveniences such as credit cards, electronic banking, and television have led to tremendous growth in mass marketing. With the growth of legitimate mass marketing, however, has come a substantial increase in fraudulent mass marketing.

Illegal mass marketers use three primary methods to identify potential victims. First, they may contact individuals with whom they have had no prior contact and attempt to scam these individuals. Second, they prompt prospective victims to contact the mass marketing operation by sending them communications that guarantee substantial awards or other benefits. Third, many mass marketers purchase lists of people who are known to have been victims of prior fraud schemes. These individuals are often receptive to investing in other schemes. Mass Marketing frauds victimize millions of Americans each year and generate losses in the hundreds of millions of dollars. The most common mass marketing schemes are:

Advanced Fee Fraud - In these scams, victims are told that they have won a lottery, received an inheritance or are otherwise entitled to a large sum of money. Often times the victim is drawn into the con by applying for a loan through a newspaper article or online advertisement placed by the con artist. Victims are informed, that in order to receive the money to which they are entitled, they must first send funds to cover taxes or processing fees.

Foreign Lottery Fraud - In Foreign Lottery Fraud, the victim is notified that he or she has won a lottery or sweepstakes but must first pay various taxes and fees before receiving the prize. The subjects, posing as lottery administrators, often send the victim a counterfeit check representing all or a portion of the victim's winnings, and require that the victim send money back to cover the taxes and fees.

Overpayment Fraud (Forged/Altered Check Scam) - Overpayment Fraud often occurs when a person advertises an item for sale in a newspaper or online. The seller is contacted by an individual wishing to purchase the item. The purchaser sends the seller a counterfeit check

for an amount greater than the price of the item and asks the seller to deposit the check and to return the remaining money or to send it to another person (often a "shipper" or "agent" who works for the purchaser).

Nigerian Letter Scam (419 Fraud) - In Nigerian Letter Scams, an e-mail, fax, or letter is sent to a

victim claiming there are millions of dollars either from an exiled head of state, political refugee, a pseudo-governmental company or a deceased relative (inheritance) in an account in a foreign country. The funds are supposedly in a security company and the victim is asked to help get the funds to the U.S. The victim is asked to wire numerous fees in conjunction with getting the funds released from the foreign country and sent to the U.S. The victim is promised a percentage of these funds for his assistance. In other cases, the victim is provided a check to pay the "fees" required, which, after the victim pays the "fees," turns out to be fraudulent. (419 Frauds are named after the Nigerian Penal Code Section 419.)

The perpetrators of mass marketing schemes generally reside outside of the U.S., while their victims are predominantly elderly U.S. citizens. As a result, the FBI is uniquely positioned to address this crime problem because of its Legal Attache Offices (Legats) located around the globe. Utilizing FBI Legats, in partnership with other foreign and domestic law enforcement agencies, the FBI has been involved in several initiatives to combat the growing problem of International Mass Marketing Fraud, including Operation Global Con (Global Con) which concluded in May 2006.

Global Con was an international initiative targeting Mass Marketing fraud schemes that were international in scope and impact, involved criminal organizations or involved significant losses. Global Con was developed by the Department of Justice (DOJ) Fraud Section, in concert with the FBI, U.S. Postal Inspection Service (USPIS), U.S. Immigration and Customs Enforcement (ICE), and the Royal Canadian Mounted Police (RCMP). Several other foreign countries participated in the initiative including Spain, the Netherlands, Nigeria, Costa Rica, the United Kingdom, and Australia.

The initiative has been extremely successful in meeting its goals of prosecution, interdiction, restitution, seizure of assets, and education of potential victims. U.S. Attorney General Gonzales called the 14-month investigation the largest enforcement operation of its kind. It resulted in 139 arrests and 61 convictions in the U.S. and an additional 426 arrests in Canada, Costa Rica, the Netherlands, and Spain. The FBI's involvement included 38 separate cases which resulted in \$16 million in forfeitures.

The FBI worked alongside the Federal Trade Commission (FTC) in the Global Con initiative. During Global Con, the FTC filed 21 federal court cases against 143 defendants, helping to stop the criminals that cost U.S. citizens more than \$150 million. In one exemplary Global Con case, the FTC was able to obtain a \$13.9 million judgment against Venezuelan and Guatemalan telemarketing fraudsters.

In addition to foreign and domestic law enforcement agencies, the FBI has also partnered with private entities like the American Association of Retired Persons (AARP) in an effort to reduce telemarketing and mass-marketing fraud. The AARP has helped limit these frauds by providing the FBI with members to act as volunteer "victims" in its investigations. The AARP also aids the FBI in its educational and awareness efforts by giving presentations to the elderly regarding fraud matters.

II. Overall Accomplishments

Through FY 2006, 147 cases investigated by the FBI resulted in 13 indictments and 44 convictions of Mass Marketing Fraud criminals. The FBI's involvement in multi-agency initiatives like Global Con has helped make significant strides in combating this fraud, as reflected in the FBI's notable statistical accomplishments as follows: \$268.8 million in Restitutions, \$86.9 million in Fines and \$12.4 million in Seizures. The chart below is reflective of the number of pending cases from FY 2002 through FY 2006. Mass Marketing cases are decreasing because of the prioritization of other white collar crime matters within the White Collar Crime Program.

III. Significant Cases

OPERATION LAST CHANCE (MEMPHIS):

Hundreds of thousands of U.S. citizens were victimized in this telemarketing scheme which purported to sell foreign lottery chances. The perpetrators collected an average of \$5 million a week at times during this scheme and laundered more than \$27 million through one bank account to disguise its origin.

Seventeen individuals residing in the U.S., Canada, Australia, Vanuatu, and Costa Rica were indicted on numerous charges relating to the scheme. In December 2002, the FBI arrested 15 individuals in the U.S., Canada, Australia, and Costa Rica. More than \$35 million located in bank accounts worldwide and personal property attributed to the defendants having been restrained. This includes the seizure of more than \$700,000 by the Australian Tax Authority. In 2005, ten individuals were convicted and \$16 million was forfeited. Of the ten individuals convicted, one was sentenced to six years incarceration, one was convicted at trial and is awaiting sentencing, and eight received probation.

PROJECT CORAL (BOSTON):

The perpetrators of this fraud were operating advance fee credit card and U.S. Federal Grants schemes. Victims were led to believe that they would receive a credit card or grant after paying the conspirators a relatively small fee. After obtaining bank account information from the victims, payments were withdrawn from their accounts via an automated clearing house but no goods or services were ever provided. It is estimated that over an 18-month period, the company defrauded over 100,000 victims for a total loss of approximately \$30 million.

In February 2005, 31 individuals were arrested, one being a former assistant manager of the HSBC Bank of New York City. Approximately \$200,000 (Canadian) and \$50,000 (US) was seized at this time. In September 2006, one of the main subjects, Stephen Clark, pled guilty to two separate conspiracy counts stemming from his role in the scheme; other subjects are currently awaiting trial. Sentencing for Clark was scheduled for January 19, 2007. This investigation was carried out by the Project COLT (Centre of Operations Linked to Telemarketing) Task Force, consisting of members of the FBI, ICE, the Royal Canadian Mounted Police (RCMP), and local law enforcement agencies.

WAYS TO PROTECT YOURSELF FROM MASS MARKETING FRAUD

Things you should do:

- Ask telemarketers for the name and address of their company and a clear explanation of the offer they are making.
- Ask the caller to send you material in writing to study, including the money back guarantee, before you make a purchase.
- Ask about the company's refund policies.
- Call the Better Business Bureau, your state Attorney General's Office, or the local Consumer Protection Service in the state or city where the company is located, and ask if any complaints have been made against the firm.
- Talk to family and friends, or call your lawyer, accountant, or banker, and get their advice

before you make any large purchase or investment.

- Request that your telephone number be removed from the telemarketing list if you do not want to be called.
- Report suspicious telemarketing calls, junk mail solicitations, or advertisements to the National Fraud Information Center at 1-800-876-7060.

Things you should NOT do:

- Do not pay for any prize or send money to improve your chances of winning--it is illegal for someone to ask that you pay to enter a contest.
- Do not allow any caller to intimidate or bully you into buying something "right now"--If the caller says, "You have to make up your mind right now," or "We must have your money today," then it's probably a scam.
- Do not give any caller your bank account number--They can use it to withdraw money from your account at any time without your knowledge and/or permission. • Do not give your credit card number to anyone over the telephone unless you initiated the call.
- Never wire money or send money by an overnight delivery service unless you initiated the transaction.

U.S. Department of Justice
Federal Bureau of Investigation

FINANCIAL CRIMES SECTION
CRIMINAL INVESTIGATIVE DIVISION

ASSET FORFEITURE/MONEY LAUNDERING

I. General Overview

The mission of the Asset Forfeiture/Money Laundering Unit (AF/MLU) is to promote the strategic use of asset forfeiture and to ensure that field offices employ the money laundering violation in all investigations, where appropriate, to disrupt and/or dismantle criminal enterprises. Following the money and then properly utilizing the asset forfeiture statutes will disrupt and dismantle criminal and/or terrorist organizations.

The AF/MLU has successfully coordinated with the Counterterrorism Division in a variety of training programs to instruct agents and task force officers how to incorporate asset forfeiture and money laundering into terrorism investigations.

The Criminal Investigative Division serves as the Program Manager for both the Asset Forfeiture Program and the Money Laundering Program, thus providing support to all FBI Investigative Programs to include International and Domestic Terrorism.

MONEY LAUNDERING

The Department of Justice defines money laundering in the following manner:

"Money laundering is the process by which criminals conceal or disguise the proceeds of their crimes or convert those proceeds into goods and services. It allows criminals to infuse their illegal money into the stream of commerce, thus corrupting financial institutions and the money supply and giving criminals unwarranted economic power."

It can be further described as follows:

A process...(a series of actions) through which income of illegal origin is concealed, disguised, or made to appear legitimate (Main objective); and to evade detection, prosecution, seizure, and taxation.

Anyway you look at it, money laundering is the process by which criminal proceeds are made to appear to come from a legitimate source. The FBI maintains a proactive approach when investigating money laundering. It is two-pronged in nature:

Prong One - The investigation of the underlying criminal activity, in simple terms, if there is no criminal activity, or Specified Unlawful Activity that generates illicit proceeds, then there can be no money laundering.

Prong Two - A parallel financial investigation to uncover the financial infrastructure of the

criminal organization. Following the money and discerning how the money flows in an organization in order to conceal, disguise, or hide the proceeds.

Asset Forfeiture

The FBI's Asset Forfeiture Program is one of the most successful in all of law enforcement. In the White Collar Crime Program (WCCP), the bulk of the monies seized are returned to victims of the frauds that generated them. This is unique to the FBI and some other agencies. Most people associate the seizure and forfeiture of assets with narcotics trafficking. Although the FBI does seize assets from drug dealers and other criminals, the WCCP is the largest contributor to the FBI's forfeiture program.

II. Overall Accomplishments:

Through FY 2006, 473 cases investigated by the FBI resulted in 161 indictments and 95 convictions of Money Laundering Fraud criminals. For FY 2006, the following Money Laundering most notable accomplishments were achieved for the White Collar Crime Program: \$17 million in Restitutions and \$3.3 million in Recoveries. The chart below is reflective of the number of pending cases from FY 2002 through FY 2006.

III. Significant Cases

MARK S. CAMARATA, DBA STRATEGIC ASSET MANAGEMENT, INC; JOHN E. NICOLO; ET AL (BUFFALO):

From approximately 1999 through 2005, a former Director of the Eastman Kodak Company devised and executed a scheme to defraud the company of over \$4 million. The Director inflated payments to vendors in exchange for illegal kickbacks. The perpetrators of the fraud included numerous independent property tax assessors and a retired undersheriff of the county. In May 2005, Nicolo was arrested on charges related to the fraud at Kodak. In addition, a search warrant was issued for Nicolo's residence and seizure warrants were executed. In total, more than \$10 million in assets were seized, including three luxury vehicles and six bank accounts.

Following Nicolo's arrest, additional investigation revealed that subject Charles Schwab, a retired tax assessor from Greece, New York, was bribed by Nicolo in efforts to reduce property assessments in that town. Schwab subsequently surrendered to the FBI after being informed of the charges against him. David Finnman, Mark Camarata's predecessor at Kodak, and Richard Ackerman, a retired Undersheriff of Yates County, were also criminally charged for their involvement in bribery schemes with Nicolo. Finnman voluntarily surrendered to the FBI. Ackerman pled guilty to various charges.

On December 8, 2005, Schwab, Nicolo, and Finnman were indicted on 42 counts related to the bribery of public officials. As of December 1, 2006, all are awaiting trial which has not been scheduled.

SIMON KARERI; NENE FALL KARERI; BOLLY BA; ROBERT ASHLEY LEE; RIGGS BANK (WASHINGTON, D.C.):

Simon Kareri, former Riggs Bank Senior Vice President, and his wife, Ndeye Nene Fall Kareri, embezzled funds from various bank accounts owned by the country of Equatorial Guinea. The

funds were then laundered through shell companies established by Kareri's wife in the British Virgin Islands. The investigation further revealed that Kareri accepted illegal kickbacks from a contractor for inflating work contracts on behalf of the Benin Embassy in Washington, D.C. In 2005, Kareri and his wife pled guilty to conspiracy, bank fraud, and money laundering. On November 16, 2006, Nene Kareri was sentenced to 75 days in prison and three years supervised release, and Simon Kareri was sentenced to 27 months in prison and four years supervised release. The FBI successfully seized more than \$1.1 million in assets as a result. The U.S. Attorney's Office declined to prosecute both Robert Ashley Lee, due to lack of evidence and Bolly Ba, who was given immunity in exchange for his testimony.

Tips and Information for Identifying Money Laundering

Know your risks and vulnerability to being used for laundering money:

- Maintain and test internal financial controls, policies, and operations.
- Know your customers and understand how their businesses operate.
- Recognize and report suspicious transactions, maintain professional skepticism.
- Beware of large-scale cash transactions, the large or rapid movement of funds, and an unrealistic net worth compared to reported income and/or employment.
- Report unusual business activity that is not financially logical or does not appear to have a legitimate economic purpose.
- Maintain good record keeping.

Educate and train employees to the symptoms of money laundering-- If a transaction appears suspicious, ask questions.

Acronyms

AARP	American Association of Retired Persons
AI	Appraisal Institute
BCBSA	Blue Cross and Blue Shield Association
BICE	Bureau of Immigration and Customs Enforcement
CAIF	Coalition Against Insurance Fraud
CFTC	Commodities Futures Trading Commission
CMS	Centers for Medicare and Medicaid Services
DCDAO	DeKalb County District Attorney's Office
DBA	Doing Business As
DEA	Drug Enforcement Agency
DOJ	Department of Justice
ESO	Executive Stock Options
FAMUPD	Florida A & M University Police Department
FDA	Food and Drug Administration
FHA	Federal Housing Authority
FIFU	Financial Institution Fraud Unit
FTC	Federal Trade Commission
FinCEN	Financial Crimes Enforcement Network
FY	Fiscal Year
HF	Hedge Fund
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HUD	Housing and Urban Development
ICE	Immigration and Customs Enforcement
IIF	Industry Insider Fraud
IPO	Initial Public Offering
IRS	Internal Revenue Service
LEGAT	Legal Attache Office
MARI	Mortgage Asset Research Institute
MBA	Mortgage Bankers Association
MEDIC	Medicare Drug Integrity Contractor
MICA	Mortgage Insurance Companies of America
NAIC	National Association of Insurance Commissioners
NAMB	National Association of Mortgage Brokers
NASD	National Association of Securities Dealers
NHCAA	National Health Care Anti-Fraud Association
NICB	National Insurance Crime Bureau
NNA	National Notary Association
OIG	Office of Inspector General
PEO	Professional Employer Organization

Acronyms (cont.)

RCMP	Royal Canadian Mounted Police
SAR	Suspicious Activity Reports
SEC	Securities and Exchange Commission
SMART	Suspicious Mortgage Activity Report Form
UCO	Undercover Operation
USAO	U.S. Attorney's Office
USPIS	U.S. Postal Inspection Service