**U. S. Department of Justice**
Federal Bureau of Investigation

**FINANCIAL CRIMES SECTION** **CRIMINAL INVESTIGATIVE DIVISION**

# FINANCIAL CRIMES REPORT TO THE PUBLIC

## FISCAL YEARS 2010 - 2011
## OCTOBER 1, 2009 – SEPTEMBER 30, 2011

## TABLE OF CONTENTS

# FINANCIAL CRIMES

**Overview and Priorities:** 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, securities and commodities fraud, health care fraud, financial institution fraud, mortgage fraud, 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.

**Mission:** 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.

In Fiscal Years (FY) 2010-2011, the FCS was comprised of the Asset Forfeiture/Money Laundering Unit (AF/MLU), the Economic Crimes Unit (ECU), the Health Care Fraud Unit (HCFU), the Forensic Accountant Unit (FAU), the Financial Institution Fraud Unit (FIFU), and the Financial Intelligence Center (FIC).

The **ECU** 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 (e.g., investment fraud schemes such as Ponzi, pyramid and advanced fee schemes; securities market manipulation schemes), and mass marketing fraud.

The **HCFU** oversees investigations targeting individuals and/or organizations who are defrauding public and private health care systems. Areas investigated under the HCFU 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 (DME) fraud, pharmaceutical drug diversion, outpatient surgery fraud, and Internet pharmacy sales.

The mission of the **FIFU** is to identify, target, disrupt, and dismantle criminal organizations and individuals who engage in fraud schemes which impact financial institutions particularly in the areas of mortgage fraud and bank failures.

The mission of the **AF/MLU** as it relates to financial institution fraud (FIF) is to identify, target, disrupt, and dismantle criminal organizations and individuals through the

strategic use of asset forfeiture; and to ensure that field offices employ the money laundering violation in all investigations, where appropriate, to assist in the disruption and/or dismantlement of criminal enterprises.

The AF/MLU also has responsibilities for the management of the Forfeiture Support Project (FSP) in Calverton, Maryland. The FSP supports the forfeiture component of all major FBI investigations through data entry and analysis of financial documents, forensic accounting, and tracing assets subject to forfeiture.

The **FAU** was established in March 2009 to support all FBI investigative matters requiring a forensic financial investigation. The FAU provides oversight of the Forensic Accountant (FoA) and Financial Analyst (FA) Programs, ensuring that the FBI's financial investigative needs and priorities are continuously addressed. Key to the FAU's mission is developing, managing, and enhancing the FoA and FA Programs, to ensure that FBI financial investigative matters are expedited with the high level of expertise required in an increasingly complex global financial system.

The **FIC** is a proactive data exploitation unit, within the FCS, created in September 2009. It is staffed with a cadre of Intelligence Analysts (IA) and Staff Operations Specialists (SOS). The FIC provides tactical analysis of financial intelligence datasets and databases, by using evolving technology and data exploitation techniques, to create targeting packages to identify or enhance the most egregious criminal enterprise investigations. The FIC has established liaison efforts with other government and private agencies to effectively address criminal threats through cooperative efforts. These partnerships will identify additional data sources to be exploited thereby increasing information sharing with our partners. Although the FIC's primary mission is to identify criminal threats, a secondary mission is to enhance ongoing investigations which involve large numbers of subjects connected to investigations in multiple field offices.

**White Collar Crime (WCC) National Priorities:** Based upon FBI field office threat strategies and directives established by the President, the Attorney General, the Director, and the Criminal Investigative Division (CID), the following national priorities for the WCC Program (WCCP) have been established: public corruption, corporate fraud/securities fraud to include Ponzi schemes, health care fraud, FIF (to include bank failures and mortgage fraud), insurance fraud, money laundering, and mass marketing fraud.

Although public corruption is a national priority within the WCCP, 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 FCS. 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 or business entity. Through the manipulation of financial data, the share price, or other valuation measurements of a corporation, financial performance may remain 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 observed an increase in the number of insider trading cases. Insider trading has been a continuous threat to the fair and orderly operation of the U.S. financial markets and has robbed the investing public of some degree of trust that markets operate fairly. The dissemination of material, non-public information commonly referred to as insider information has also caused irreparable harm to victim institutions whose employees illegally pass privileged corporate information. The FBI has worked extensively with the U.S. Securities and Exchange Commission (SEC) to target the widespread problem of insider trading which has plagued the fair and orderly operation of the securities markets.

Additionally, corporate fraud matters involving self-dealing by corporate executives, particularly utilizing companies to perpetrate large-scale, high-yield fraud schemes, continue to be an issue of concern. Traditionally, Ponzi schemes were perpetrated by individuals or small groups within a community environment. However, the current financial crisis resulted in the exposure of several large Ponzi schemes (e.g. Petters Worldwide investigation) perpetrated not on an individual community level, but on a corporate national level by executives of what were once considered legitimate companies.

The FBI continues to address corporate fraud cases specifically involving subprime lending institutions, brokerage houses, home-building firms, hedge funds and financial institutions, as a result of the financial crisis partly caused by the collapse of the subprime mortgage market in the fall of 2007. As a result of the current financial crisis, trillions of dollars in shareholder value were lost, several prominent companies went out of business, several prominent banks failed, and the Federal Government provided over a trillion dollars in relief to keep other companies from failing.

A subprime mortgage lender is a business that lends to borrowers who do not qualify for loans from mainstream lenders. Once the subprime loans have been issued, they are bundled and sold as securities -- a process known as securitization. Fraud has been identified throughout the loan process, which commences with the borrower providing false information to the mortgage broker and/or lender. The next layer of potential fraud, the corporate fraud, occurs with the banks, brokerage houses, and other financial institutions that package loans through the securitization process. As the housing market declined, subprime lenders have been forced to buy back a number of nonperforming loans. Many of these subprime lenders have relied on a continuous increase in real estate values to allow the borrowers to refinance or sell their properties before going into default. However, based on the sales slowdown in the housing market, loan defaults increased, the secondary market for subprime securities dwindled, and the securities lost value. As a result, publicly traded stocks dramatically decreased in value as financial institutions realized large losses due to the subprime securities they held or insured, resulting in financial difficulties and bankruptcies. After experiencing a dramatic rise in cases during FY 2009, the number of investigations pertaining to the subprime industry has remained relatively stable during the last two years.

As publicly traded companies suffered financial difficulties due to subprime market losses, analyses of company financials have identified instances of false accounting entries and fraudulently inflated assets and revenues. Investigations have determined that several of these companies manipulated their reported loan portfolio risks and used various accounting schemes to inflate their financial reports. Additionally, before these companies' stocks rapidly declined in value, executives with insider information sold their equity positions and profited illegally. The FBI continues to coordinate with the U.S. Department of Justice (DOJ), the SEC, and other U.S. law enforcement and regulatory agencies to identify and address possible corporate fraud.

Corporate fraud remains one of the highest priorities in CID. At the end of FY 2011, 726 corporate fraud cases were being pursued by FBI field offices throughout the United States, several of which involved losses to public investors that individually exceed $1 billion.

Corporate fraud investigations involve the following activities:

(1) Falsification of financial information of public and private corporations, including:

(a) False accounting entries and/or misrepresentations of financial condition;
(b) Fraudulent trades designed to inflate profit or hide losses; and
(c) Illicit transactions designed to evade regulatory oversight.

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

(a) Insider trading- trading based on material, non-public information, including, but not limited to:
a. Corporate insiders leaking proprietary information;

b. Attorneys involved in merger and acquisition negotiations leaking info;
c. Matchmaking firms facilitating information leaks;
d. Traders profiting or avoiding losses through trading; and
e. Payoffs or bribes in exchange for leaked information.

(b) Kickbacks;
(c) Misuse of corporate property for personal gain; and
(d) Individual tax violations related to self-dealing.

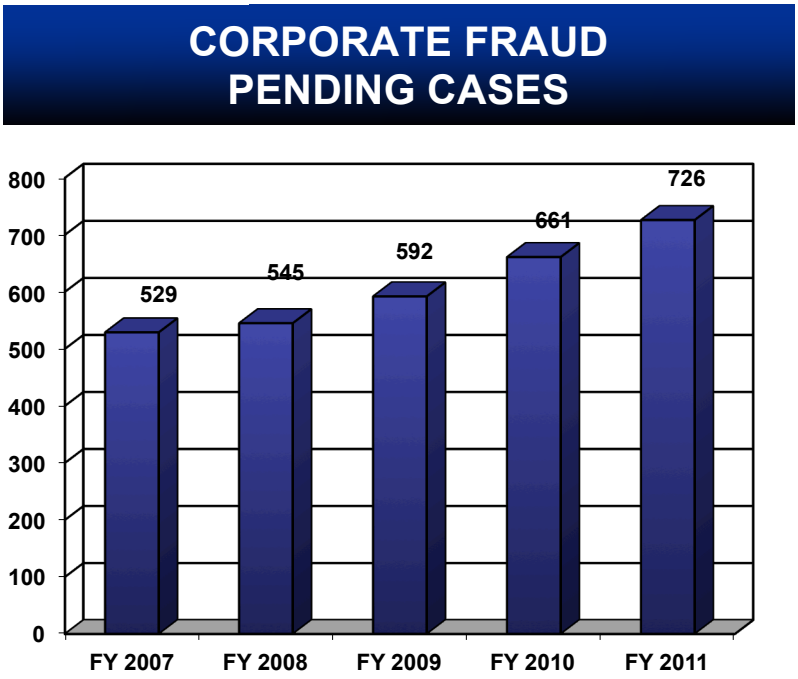
(3) Obstruction of justice designed to conceal any of the above-noted types of criminal conduct, particularly when the obstruction impedes the inquiries of the SEC, other regulatory agencies, and/or law enforcement agencies.

The FBI has formed partnerships with numerous agencies to capitalize on its 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, Financial Industry Regulation Authority (FINRA), Internal Revenue Service (IRS), Department of Labor, Federal Energy Regulatory Commission, Commodity Futures Trading Commission (CFTC), U.S. Postal Inspection Service (USPIS), and Special Inspector General for the Troubled Asset Relief Program (SIGTARP), among others. In September 2010, the FBI executed a Memorandum of Understanding with the SEC and placed a Supervisory Special Agent within the SEC's Office of Market Intelligence in order to facilitate cooperation in a variety of financial investigations. This assignment has facilitated case referrals between both agencies. In addition, the FBI is an active member of the Financial Fraud Enforcement Task Force (FFETF) created by Presidential Executive Order in November 2009. As reflected in the statistical accomplishments of the FBI, the cooperative and multiagency 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, Association of Certified Fraud Examiners, and the North American Securities Administrators 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 and Dun & Bradstreet have been able to provide significant background information on subject individuals and/or subject companies to further investigative efforts.

## II. Overall Accomplishments

During FY 2011, cases pursued by the FBI resulted in 242 indictments/informations and 241 convictions of corporate criminals. Numerous cases are pending plea agreements and trials. During FY 2011, the FBI secured $2.4 billion in restitution orders and $16.1 million in fines from corporate criminals. The chart below reflects corporate fraud pending cases from FY 2007 through FY 2011:




## III. Significant Cases

**Beazer Homes (Charlotte):** A subprime-related corporate fraud investigation conducted by the Charlotte Field Office recently culminated in the trial conviction of the former Chief Accounting Officer of Beazer Homes USA (Beazer). Executives at Beazer, a former Fortune 500 company located in Charlotte, North Carolina, encouraged the use of false information to finance and sell homes and to manipulate corporate earnings to meet specific goals. This manipulation of earnings, referred to as cookie jar accounting, allowed Beazer to reduce their net income during strong financial periods and provide them with excess balances and reserves allowing them to "smooth earnings" during times of underperformance. On July 1, 2009, Beazer entered into a Deferred Prosecution Agreement (DPA) acknowledging corporate culpability in this complex fraud scheme. As part of the DPA, Beazer agreed to pay restitution of $50 million and continued to cooperate with the government's criminal investigation of former Beazer executives. On October 28, 2011, Michael Rand, the former Chief Accounting Officer of Beazer, was convicted on 7 of 11 counts after a three-week trial. Sentencing is planned for 2012.

**Colonial Bank and Taylor, Bean & Whitaker (Washington, D.C.):** Another notable success was the sentencing of multiple executives from Colonial Bank and Taylor, Bean & Whitaker (TBW). The Washington Field Office investigated a subprime-related conspiracy committed by senior executives at Colonial Bank and TBW, a major U.S. mortgage originator, who conducted a several billion-dollar accounting fraud through back-dating of loans and the creation of fictitious loans which inflated loan asset values. Additionally, Colonial Bank fraudulently sought to acquire $553 million in TARP funds which was prevented by the FBI in conjunction with the SIGTARP. In August 2009, TBW closed after it could no longer issue government-backed loans. In August 2009, the Alabama State Banking Department closed Colonial Bank due to liquidity problems. The failure of Colonial Bank represents the sixth-

largest bank failure since the creation of the Federal Deposit Insurance Corporation (FDIC). Colonial Bank's former Senior Vice President Cathy Kissick and TBW Chief Executive Officer Paul Allen pled guilty and in June 2011, were sentenced to eight years and 40 months in prison, respectively. In April 2011, after a ten-day trial, a jury found former TBW Chairman Lee Farkas, guilty on 14 counts of bank fraud, wire fraud, and securities fraud. Farkas was later sentenced to 30 years' imprisonment.

**Galleon Group (New York):** The New York Field Office conducted multiple investigations into insider trading. Targets of this investigation included Wall Street analysts and insiders, lawyers, hedge fund analysts and traders, company insiders, and professional consulting firms. Insiders from corporations such as McKinsey & Company, International Business Machines, Advanced Micro Devices, and Goldman Sachs have been charged for the unauthorized release of proprietary corporate information. The most prominent individual convicted in the investigation to date is Raj Rajaratnam, the founder of the $7 billion Galleon Group hedge fund. Mr. Rajaratnam was convicted in May 2011 by a federal jury on all 14 counts he faced pertaining to his insider trading activity and was subsequently sentenced to 11 years' imprisonment. This investigation has shown the FBI's propensity to use all tools available at its discretion, including Title IIIs, to combat financial crimes. As of September 30, 2011, 48 convictions have been obtained in this wide-ranging FBI probe into illicit insider trading activity on Wall Street and in the boardrooms across the United States.

# SECURITIES AND COMMODITIES FRAUD

## I. General Overview

The continued uncertainty and volatility of today's financial markets could be measured by the Dow Jones Industrial Average movement from 12,681 on July 22, 2011, to 10,655 on October 3, 2011. As a result of such tumultuous markets, the FBI witnessed a steady rise in securities and commodities frauds as investors sought alternative investment opportunities. With the development of new schemes and trends, such as securities market manipulation via cyber intrusion, the increase in commodities fraud, the continued rise of Ponzi schemes and foreign-based reverse merger market manipulation schemes, securities and commodities fraud is on the rise. Since 2008, securities and commodities fraud investigations have increased by 52 percent, and the FBI currently has over 1,800 pending investigations. During this period, the losses associated with these types of schemes have increased to billions of dollars. The losses are associated with depreciative market value of businesses, reduced or nonexistent 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, pension funds, and retirement funds.

The continuing integration of global capital markets has created unprecedented opportunities for U.S. businesses to access capital and investors to diversify their portfolios. Whether through individual brokerage accounts, college savings plans, or retirement accounts (e.g. 401k plans), more and more Americans are choosing to invest in the U.S. securities and commodities markets. This growth has led to a corresponding growth in the amount of fraud and misconduct seen in these markets. The creation of complex investment vehicles and the tremendous increase in the amount of money being invested have created greater opportunities for individuals and businesses to perpetrate fraudulent investment schemes. The recent financial crisis led to the identification of numerous investment fraud schemes, many which were Ponzi schemes. The number of investment frauds continues to grow as investors remain susceptible in the current uncertainty of the global economy. The securities and commodities frauds being investigated include market manipulation, investment frauds, and miscellaneous matters such as broker embezzlement. In response to this growing threat, the FBI has increased the number of agents addressing it by 61 percent, an increase of approximately 91 agents since 2008.

Additionally, the FBI works closely with various governmental and private entities to investigate and prevent fraudulent activity in the financial markets. In an effort to 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), CFTC, FINRA, USPIS, and the IRS, among others serving as force multipliers to more effectively address the securities and commodities fraud threat. Nationally,

the FBI participates in several working groups and task forces such as the FFETF. The FFETF was established by President Obama to coordinate the efforts of the DOJ at all levels of government to disrupt and dismantle significant large-scale criminal enterprises.

Valuable partnerships have been instrumental in orchestrating national financial crimes takedowns, or "sweeps," during the last few years. By coordinating fraud cases into a nationwide takedown, the FBI and its partners have raised public awareness of its enforcement efforts and deterred future fraud. Operation Broken Trust (OBT) was a multiagency national initiative which coordinated the efforts of government agencies against various securities fraud threats. OBT featured criminal, civil, and community outreach components. The sweep targeted individuals and companies who engaged in criminal and civil securities fraud which occurred sometime from August 16, 2010, through December 1, 2010. For the criminal component coordinated by the FBI, this included arrests, complaints, information/indictments, convictions, sentences, and seizures/forfeitures. The focus of the sweep was schemes to defraud individual investors, affinity fraud, prime bank fraud, commodities frauds, and market manipulation cases, such as "pump and dump" schemes.

On December 6, 2010, the FFETF - Securities Fraud Working Group held a national press conference to announce the conclusion of OBT. U.S. Attorney General Eric Holder gave remarks on behalf of DOJ. In coordination with the national press conference, local press conferences were held across the country by U.S. Attorneys participating in the operation. The operation involved 343 criminal defendants nationwide and more than 120,000 victims with losses attributable to alleged criminal activity of more than $8 billion.

Following are the most prevalent types of securities and commodities fraud:

**Investment Fraud:** These schemes, sometimes referred to as High Yield Investment Fraud, involve the illegal sale or purported sale of financial instruments. Financial instruments are defined broadly as any contract that gives rise to a financial asset of one entity and a financial liability or equity instrument to another entity. These instruments can be a tradable asset of any kind to include registered securities and commodities, and unregistered securities (e.g. a simple promissory note between the fraudster and his/her victim investors). Schemes take on many forms and perpetrators quickly alter schemes as they are thwarted by law enforcement. The typical investment fraud schemes are characterized by offers of low- or no-risk investments, guaranteed returns, overly consistent returns, complex strategies, or unregistered securities. These schemes often seek to victimize affinity groups, such as a group with a common religion or ethnicity, to utilize the common interests to build trust to effectively operate against them the investment fraud. The perpetrators range from professional investment advisors and hedge funds to those you put your trust in and interact daily with such as a neighbor or sports coach. The fraudster's ability to foster trust makes these schemes so successful, and investors should use scrutiny and gather as much information as possible before entering into any new investment opportunities. Investors can find background information on registered investment advisors at www.sec.gov and registered brokers and brokerage firms at www.finra.org. The following are additional definitions of the most common investment fraud scheme variations:

**Ponzi Schemes** - A Ponzi scheme is an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors. Ponzi schemes often share common characteristics such as offering overly consistent returns, unregistered investments, high returns with little or no risk, or secretive or complex strategies. This arrangement gives investors the impression there is a legitimate, money-making enterprise behind the subject's story, but in reality, unwitting investors are the only source of funding.

**Affinity Frauds** - Perpetrators of affinity frauds take advantage of the tendency of people to trust others with whom they share similarities such as religion or ethnic identity to gain their trust and money.

**Pyramid Schemes** - 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 scheme.

**Prime Bank Investment Fraud** - In these schemes, perpetrators claim to have access to a secret trading program endorsed by large financial institutions such as the Federal Reserve Bank, Treasury Department, World Bank, International Monetary Fund, etc. Perpetrators often claim 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 the investments are insured against loss.

**Advance Fee Fraud** - Advance fee schemes require victims to advance relatively small sums of money in the hope of realizing much larger gains. Not all advance fee schemes are investment frauds. In those that are, however, victims are told that in order to have the opportunity to be an investor (in an initial offering of a promising security, investment or commodity, etc.), the victim must first send funds to cover taxes or processing fees, etc.

**Promissory Notes** - These are generally short-term debt instruments issued by little-known or nonexistent companies. The notes typically promise high returns with little or no risk and are typically not registered as securities with the appropriate regulatory agency.

**Commodities Fraud** - Commodities fraud is the sale or purported sale of a commodity through illegal means. Commodities are raw materials or semifinished goods that are relatively uniform in nature and are sold on an exchange (e.g., gold, pork bellies, orange juice, and coffee). Most commodities frauds involve illicit marketing or trading in commodities futures or options. Perpetrators often offer investment opportunities in the commodities markets that falsely promise high rates of return with little or no risk. Two common types of commodities investment frauds include the following:

**Foreign Currency Exchange (Forex) Fraud** - The perpetrators of Forex frauds entice individuals into investing in the spot foreign currency market through false claims and high-pressure sales tactics. Foreign currency firms that engage in this type of fraud invest client funds into the Forex market, not with the intent to conduct a profitable trade for the client but merely to “churn” the client’s account. Churning creates large commission charges

benefiting the trading firm. In other Forex frauds, the perpetrator creates artificial account statements that reflect purported investments when, in reality, no such investments have been made. Instead, the money has been diverted for the perpetrator's personal use.

**Precious Metals Fraud** - These fraud schemes offer investment opportunities in metals commodities such as rare earth, gold, and silver. The perpetrators of precious metals frauds entice individuals into investing in the commodity through false claims and high-pressure sales tactics. Oftentimes in these frauds, the perpetrators create artificial account statements that reflect purported investments when, in reality, no such investments have been made. Instead, the money has been diverted for the perpetrators' personal use.

**Market Manipulation:** These schemes, commonly referred to as "Pump and Dumps," are effected by creating artificial buying pressure for a targeted security, generally a low-trading volume issuer in the over-the-counter securities market that is largely controlled by the fraud perpetrators. This artificially increased trading volume has the effect of artificially increasing the price of the targeted security (i.e., the Pump), which is rapidly sold off into the inflated market for the security by the fraud perpetrators (i.e., the Dump). These actions result in illicit gains to the perpetrators and losses to innocent third-party investors. Typically, the increased trading volume is generated by inducing unwitting investors to purchase shares of the targeted security through false or deceptive sales practices and/or public information releases.

A modern variation on these schemes involves largely foreign-based computer criminals gaining unauthorized access and intruding into the online brokerage accounts of unsuspecting victims in the United States. These intruded victim accounts are then utilized to engage in coordinated online purchases of the targeted security to affect manipulation, while the fraud perpetrators sell their preexisting holdings in the targeted security into the inflated market.

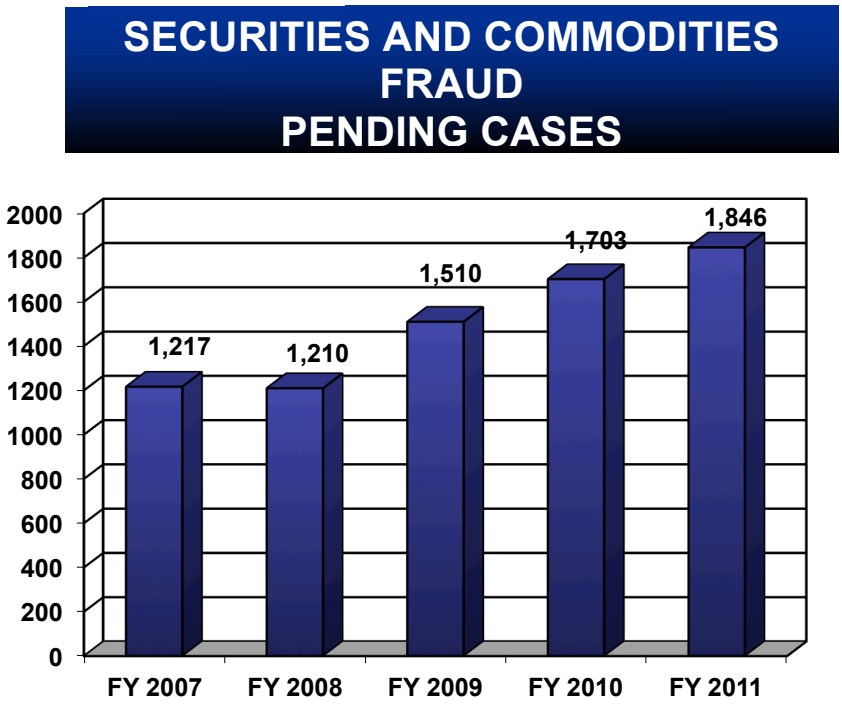
**Broker Embezzlement:** These schemes involve illicit and unauthorized actions by brokers to steal directly from their clients. Such schemes may be facilitated by the forging of client documents, doctoring of account statements, unauthorized trading/funds transfer activities, or other conduct in breach of the broker's fiduciary responsibilities to the victim client.

**Late-Day Trading:** These schemes involve the illicit purchase and sale of securities after regular market hours. Such trading is restricted in order to prevent individuals from profiting on market-moving information which is released after the close of regular trading. Unscrupulous traders attempt to illegally exploit such opportunities by buying or selling securities at the market close price, secure in the knowledge that the market-moving information will generate illicit profits at the opening of trading on the following day.

## II. Overall Accomplishments

As of the end of FY 2011, the FBI was investigating 1,846 cases of securities and commodities fraud and had recorded 520 indictments/informations and 394 convictions against this criminal threat. Additional notable accomplishments in FY 2011 include: $8.8 billion in restitution orders; $36 million in recoveries; $113 million in fines; and $751 million in

forfeitures. The chart below reflects securities and commodities fraud pending cases from FY 2007 through FY 2011:




**III. Significant Cases**

**Joseph Blimline, Provident Royalties (Dallas):** This investigation centered on Joseph Blimline who orchestrated one of North Texas' largest oil and gas investment Ponzi schemes defrauding 7,700 investors of over $485 million. Beginning in 2006, Blimline and others involved at Provident Royalties made false representations and failed to disclose other material facts to their investors. The investors were not told that Blimeline had received millions of dollars of unsecured loans and had been previously charged with securities fraud. Blimline issued approximately 20 oil and gas offerings raising over several hundred million dollars from investors. Blimline used a significant amount of the money raised in these offerings to purchase oil and gas assets from earlier offerings and to pay dividends to earlier investors to facilitate the scheme. On August 31, 2010, Blimline pled guilty to an Information. Blimline is awaiting sentencing in January 2012.

**A & O Entities (Richmond):** A&O originally sold fractionalized, no-risk interests in life insurance policies primarily to elderly investors with promised rates of return from 9-15 percent. A&O bank accounts were under the control of the owners of A&O, who diverted more than $50 million for their personal benefit. This case was investigated jointly with the Virginia Financial and Securities Fraud Task Force. On September 27, 2011, coconspirator Chris Allmendinger was sentenced to 45 years' imprisonment for his role in the scheme. On September 28, 2011, Adley Adulwahab was sentenced to 60 years' imprisonment, which is the second-longest white collar criminal sentence in the history of the Eastern District of Virginia.

As of September 30, 2011, seven subjects have been sentenced to federal prison terms ranging from three years to 60 years for their roles in a Ponzi scheme that bilked more than 800 investors, mostly elderly, of more than $100 million.

**Nicholas Cosmo (New York):** Nicholas Cosmo was the owner and President of Agape World, Inc. and Agape Merchant Advance LLC (AMA). Cosmo, through Agape and AMA, solicited money from investors purportedly to provide bridge loans to companies. Cosmo, and his sales force, promised investors returns of 12 to 15 percent per month. The investor funds were ultimately used to pay Cosmo's personal expenses, pay back previous investors, and speculate in future contracts. In April 2009, Nicholas Cosmo was indicted on charges of mail fraud in connection with operating a several hundred million-dollar Ponzi scheme. On October 14, 2011, Cosmo was sentenced to 25 years of imprisonment by U.S District Court Judge Denis R. Hurley in federal court in Central Islip. Cosmo was ordered to pay $179 million in restitution to more than 4,000 victims and agreed to an asset forfeiture judgment in the amount of $409,305,000 as part of his sentence.

# HEALTH CARE FRAUD

## I. General Overview

The FBI's mission in health care fraud (HCF) is to oversee the FBI's HCF initiatives by providing national guidance and assistance to support HCF investigations targeting individuals and organizations who are defrauding the public and private health care systems. The FBI, 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, works 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 three and ten percent of total health care expenditures. The fraud schemes are not specific to any area, but they 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.

**Emerging Trends and Projections:** HCF 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 that total health care expenditures are estimated to total $2.4 trillion, representing 14 percent of the Gross Domestic Product (GDP). By the year 2016, CMS estimates total health care spending to exceed $4.14 trillion, representing 19.6 percent of the GDP.

With health care expenditures consistently increasing, 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 HCF 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 Health and Human Services-Office of

Inspector General (HHS-OIG), the Food and Drug Administration (FDA), Drug Enforcement Administration, Defense Criminal Investigative Service, Office of Personnel Management, IRS-CID, 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, the National Insurance Crime Bureau (NICB), as well as many other professional and grass-roots efforts to expose and investigate fraud within the system.

**Collaboration:** In furtherance of the FBI's efforts to combat HCF in the United States, 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 coordination meetings at the DOJ which includes various DOJ components involved in the fight against HCF. National-level liaison is also maintained with federal law enforcement agencies, the National Association of Medicaid Fraud Control Units, and other partners.

Throughout the country, FBI field offices participate in HCF Working Groups which involve law enforcement agencies, prosecutors, regulatory agencies, and health insurance industry professionals to identify the various crime problems involving HCF. 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.

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 DME, hospital fraud, physician fraud, home health agencies, beneficiary-sharing, chiropractic, pain management, and associated drug diversion, physical therapists, prescription drugs, multidisciplinary 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 HCF, the FBI cooperates with the DOJ and the various USAOs 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 HCF 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.

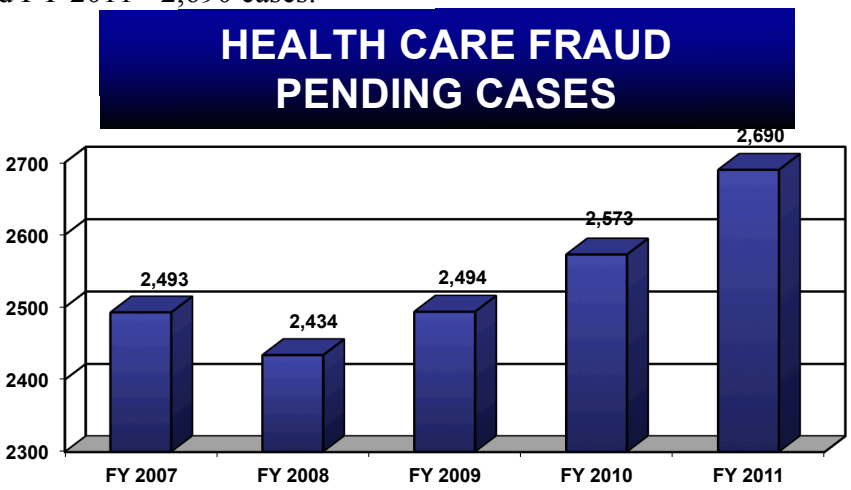
**Data Mining Techniques:** The FBI and the health care industry continue to expand their technology and intelligence assessments through the use of sophisticated data-mining techniques to identify patterns of fraud, systemic weaknesses, and aberrant billing activity.

In 2005, the FCS developed the Electronic Bank Records Initiative (EBRI). The EBRI was implemented to identify and develop a process for obtaining electronic (digital format) records from financial institutions. Historically, financial institutions have provided paper copies of records to law enforcement when they receive a subpoena from the government. These records are generally maintained by the banks in an electronic format. The time it takes the financial institution to make the copies of the records and for the investigative agencies to return the paper copies back to an electronic format for financial analysis creates a severe negative effect on the timeliness, effectiveness, and efficiency of investigations. In an effort to increase the efficiency of the process, a subpoena attachment was developed by the DOJ, FBI, and the IRS-CID for the production of electronic records instead of paper copies. The development included significant coordination with the financial institutions and their associations. The subpoena attachment was not based upon new or expanded laws, regulations, or rules. The attachment is merely meant to standardize and clarify the requests for electronic records according to the current Federal Rules of Criminal and Civil Procedure. In general terms, if a financial institution maintains records electronically, the requesting agency would be seeking to obtain the records electronically. In addition, the scope of the records requested has not changed due to the subpoena attachment, with the exception of seeking the records electronically.

The subpoena attachment was disseminated to FBI offices, IRS offices, and throughout the DOJ in November 2007. The goal of the DOJ, FBI, and IRS-CID is to inform and prepare financial institutions and their respective agencies for the use and response to the subpoena attachment. This includes working with financial institutions during the transition period in coordinating the requests and associated responses to subpoenas. In addition, it is anticipated the EBRI will greatly increase the efficiency of the financial records production process and provide significant costs savings to both the government and private industry.

## II. Overall Accomplishments

Through FY 2011, 2,690 cases investigated by the FBI resulted in 1,676 informations/indictments and 736 convictions of HCF criminals. It should be noted that numerous cases are pending plea agreements and trials. The following notable statistical accomplishments are reflective in FY 2011 for HCF: $1.2 billion in restitutions, $1 billion in fines, $96 million in seizures, $320 million in civil restitution, and over $1 billion in civil settlements. The chart below reflects HCF pending cases from FY 2007 through FY 2011 as follows: FY 2007 - 2,493 cases; FY 2008 - 2,434 cases; FY 2009 - 2,494 cases; FY 2010 - 2,573 cases; and FY 2011 - 2,690 cases.



## III. Significant Cases

**Glaxosmithkline (GSK) (San Juan):** Drugs manufactured at the GSK plant located in Cidra, Puerto Rico, were not safe and/or effective and, therefore, claims for payment of prescription drugs made by GSK to Medicare, state Medicaid programs, and other state and federal purchasers of prescription drugs were false or fraudulent. GSK is accused of distributing reject drug product to the U.S. market and the submission of false claims for drug products that were not safe and/or effective. Drugs affected include, but are not limited to, Avandamet, Coreg, Bactroban, Abreva, Cimetidine, and Kytril. GSK allegedly lied to the FDA in order to conceal those violations. GSK's violations of Current Good Manufacturing Practices include, but are not limited to, product mix-ups; inadequate investigation of out-of-specification results detected during laboratory testing; inadequate process validation and equipment calibration; and substandard quality and control of the plant's water systems, resulting in microbial contamination of drug products. On December 26, 2010, GSK pled guilty to charges relating to the manufacture and distribution of certain adulterated drugs. A $600 million civil settlement under the False Claims Act was agreed upon in addition to $150 million in criminal fines and forfeiture.

**American Therapeutic Corporation (Miami):** This matter was initiated by a civil qui tam filed unsealed by a relator. The investigation into American Therapeutic Corporation (ATC) addressed an identified threat of community mental health center fraud within South Florida. This investigation is being worked jointly by FBI Miami and HHS-OIG, along with trial attorneys from DOJ. ATC has been identified as the largest Community Medical Health Center (CMHC) within Florida, and their owners and operators of facilities have submitted approximately $205 million in fraudulent claims to Medicare with approximately $85 million being reimbursed. ATC owners allegedly have been engaged in widespread fraud and paying kickbacks to assisted living facilities in order to recruit patients for unnecessary group therapy programs and partial hospitalization programs. This investigation has brought greater awareness to the fraud and abuse of CMHCs within South Florida. Payments to ATC have been suspended thereby protecting the federal trust fund for Medicare. On September 16, 2011, owner Lawrence Duran was sentenced to 50 years in prison and restitution of $87,533,863. On September 19, 2011, owner Marianella Valera was sentenced to 35 years in prison and restitution of $87,533,863. Over 20 defendants were indicted and arrested as part of the investigation.

## IV. Health Care Fraud Schemes

HCF 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 on the claim so that the health insurer will not realize 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 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 a 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.

## V. Health Care Fraud Prevention Measures

HCF is not a victimless crime. It increases health care costs for everyone. It is as dangerous as identity theft. Fraud has left many thousands of people injured. Participation in HCF 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 attracts 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, such as your "explanation of benefits," after receiving health care services. Check to ensure the dates and services are correct to ensure you get what you paid for.
- If you suspect HCF, contact your insurance company. You can also contact your local FBI field office and/or the local Department of HHS-OIG Office.

# MORTGAGE FRAUD

## I. General Overview

The mission of the Financial Institution Fraud Unit (FIFU) is to oversee the investigation of financial industry fraud schemes perpetrated by individuals, as well as criminal organizations, which target our nation's financial institutions.

The FIFU protects the public's interest by educating individuals and businesses about pervasive financial industry fraud schemes; working closely with federal, state, and local law enforcement agencies; and maintaining liaison contacts with our regulatory and industry partners. In addition, the FIFU obtains relevant intelligence data to prepare proactive strategies to neutralize current and emerging financial threats. The FIFU has oversight responsibilities of the mortgage fraud, financial institution fraud, credit card fraud, and bankruptcy fraud subprograms.

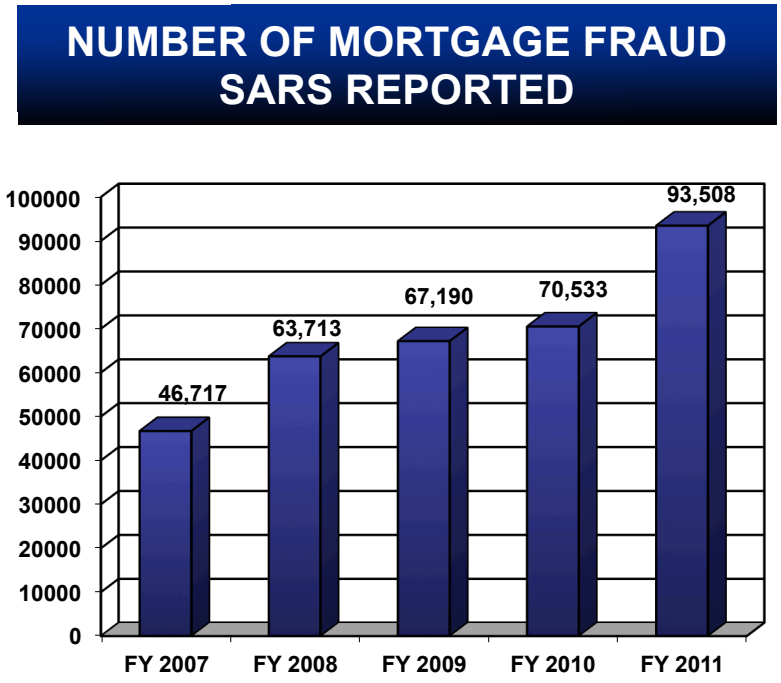
In 2011, mortgage loan originations were at their lowest levels since 2001. This can be partially attributed to tighter underwriting standards following the financial crisis. This decrease in loan originations has resulted in a corresponding decrease in new loan origination fraud investigations. Foreclosures and delinquencies, on the other hand, have skyrocketed over the past few years, with a corresponding increase in mortgage fraud schemes aimed at distressed homeowners. For the first time in recent history, distressed homeowner fraud has displaced loan origination fraud as the number one mortgage fraud threat in many offices. Though the FBI considers loan origination fraud to be the most egregious type of mortgage fraud because of the high-dollar losses attendant therewith, the FBI has now adapted its focus to include other new and emerging schemes.

Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction. These schemes include:

- Foreclosure Rescue Schemes
- Loan Modification Schemes
- Illegal Property Flipping
- Builder Bailout/Condo Conversion
- Equity Skimming
- Silent Second
- Home Equity Conversion Mortgage (HECM)
- Commercial Real Estate Loans
- Air Loans

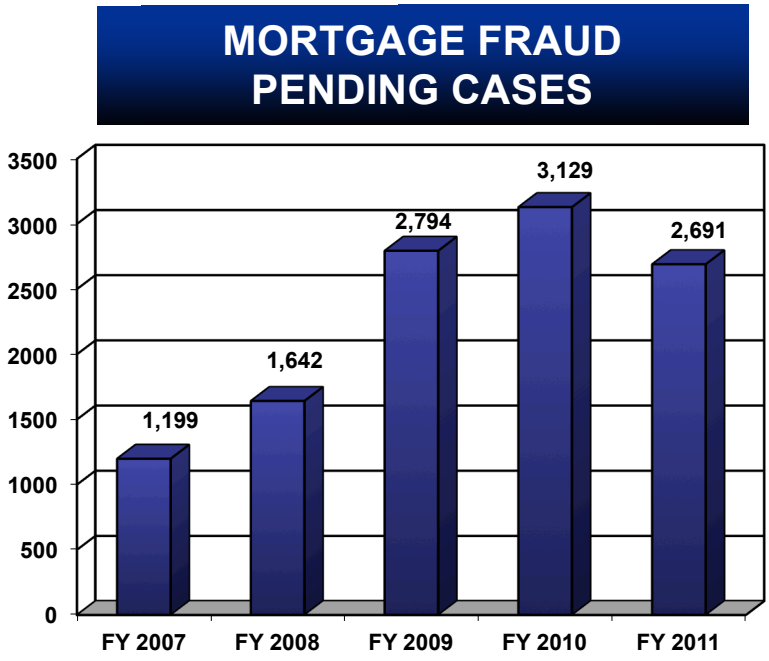
Mortgage fraud is a part of the FIF subprogram within the FBI's WCCP. The FBI investigates mortgage fraud in two distinct areas: Fraud for Profit and Fraud for Housing. Those who commit mortgage fraud for profit are often industry insiders using their specialized knowledge or authority to commit or facilitate the fraud. Current investigations and widespread reporting indicate a high percentage of mortgage fraud involves collusion by industry insiders, such as bank officers, appraisers, mortgage brokers, attorneys, loan originators, and other professionals engaged in the industry. Fraud for Housing typically represents illegal actions conducted solely by the borrower, who is motivated to acquire and maintain ownership of a house under false pretenses such as misrepresented income and asset information on a loan application.

One of the ways the FBI becomes aware of mortgage fraud is through the analysis of Suspicious Activity Reports (SARs), which are filed by federally insured financial institutions. Mortgage fraud SARs have increased from 6,936 in FY 2003 to 93,508 in FY 2011. These SARs provide valuable intelligence in mortgage fraud trends and can lead to the initiation of mortgage fraud cases, as well as the enhancement of current FBI investigations.




Note: Of those SARs that report a dollar loss, approximately 82 percent do not contain a dollar loss amount.

**FBI Response:** With elevated levels of mortgage fraud, the FBI has continued to dedicate significant resources to the threat. The FBI has increased the number of agents who investigate mortgage fraud cases from 120 Special Agents in FY 2007 to 325 Special Agents in FY 2011. FBI pending mortgage fraud cases have increased from 1,199 in FY 2007 to 2,691 in FY 2011, with a peak of 3,129 in FY 2010.



The FBI employs advanced and/or sophisticated investigative techniques, such as undercover operations and wiretaps, which result in the collection of valuable evidence and provide an opportunity to apprehend criminals in the commission of their crimes. This ultimately reduces the losses to individuals and financial institutions. The FBI has also instituted several intelligence initiatives to support mortgage fraud investigations and has improved law enforcement and industry relationships. The FBI has established methodology to proactively identify potential mortgage fraud targets using tactical analysis coupled with advanced statistical correlations and computer technologies.

In September 2009, the FBI established the FIC to provide tactical analysis of intelligence datasets and financial databases. The FIC uses evolving technology and data exploitation techniques to create targeting packages to identify the most egregious criminal enterprises and to enhance current criminal investigations. The FIC has worked jointly with the FIFU to assist the field offices by creating mortgage fraud targeting packages.

The FBI continues to enhance liaison partnerships within the mortgage industry and law enforcement to promote mortgage fraud awareness and share intelligence. As part of the effort to address mortgage fraud, the FBI continues to support 25 mortgage fraud task forces and 67 working groups. The FBI also participates in the DOJ National Mortgage Fraud and National Bank Fraud Working Groups, as well as the FFETF. The FFETF's mission is to enhance the government's effectiveness in sharing information to help prevent and combat financial fraud. FBI personnel routinely participate in various mortgage industry conferences and seminars, including those sponsored by the Mortgage Bankers Association (MBA). Collaborative educational efforts are ongoing to raise public awareness of mortgage fraud schemes through the publication of the annual Mortgage Fraud Report and this report, and through the dissemination of information jointly or between various industry and consumer organizations. Analytic products are routinely distributed to a wide audience, including public and private sector industry partners, the intelligence community, and other federal, state, and local law enforcement partners.

In June 2010, Operation Stolen Dreams was the largest collective enforcement effort ever brought to bear in confronting mortgage fraud. This FIFU-led initiative involved 1,517 criminal defendants nationwide, who were allegedly responsible for more than $3 billion in losses. Additionally, the operation resulted in 191 civil enforcement actions and the recovery of more than $196 million.

The FBI remains committed to its responsibility to aggressively investigate mortgage fraud, as well as engage with the mortgage industry in identifying fraud trends and educating the public. To maximize current resources, the FBI is relying on intelligence collection and analysis to identify emerging trends and egregious offenders and strong relationships with law enforcement and regulatory agency partners to disrupt and dismantle the criminal organizations and individuals engaging in these fraud schemes.

## II. Overall Accomplishments

Through FY 2011, FBI investigations resulted in 1,223 informations and indictments and 1,082 convictions of mortgage fraud criminals. The following notable statistical accomplishments are reflective in FY 2011 for mortgage fraud: $1.38 billion in restitutions, $116.3 million in fines, seizures valued at $15.7 million, and $7.33 million in forfeitures.

## III. Significant Cases

**Luis Belevan, The Guardian Group, LLC (Phoenix):** Luis Belevan pled guilty in federal court to conspiring to commit wire fraud and mail fraud during the period of 2009 to 2010. Belevan and his coconspirator, were charged with defrauding at least 1,800 local distressed homeowners out of a $1,595 upfront fee for bogus promises of assistance in avoiding home foreclosure. Belevan used false promises on the company's website to convince consumers that it could help them save their home, if the homeowner paid an upfront fee. The homeowners were never helped, and they were scammed out of their hard-earned money. Belevan generated almost $3 million in funds in just nine months, which he and others used for personal expenses and for other failed ventures.

**Howard Shmuckler, The Shmuckler Group (Washington, D.C.):** From 2009 to 2010, Howard Shmuckler owned and operated a mortgage-rescue business known as The Shmuckler Group (TSG), which claimed to be the "largest, most successful group of professionals…coming together to help home owners keep their homes in a manageable and affordable manner." Operating his business at various times in McLean and Vienna, Virginia, Shmuckler is accused of misrepresenting that TSG had a success rate of 97 percent and falsely portraying himself as an attorney licensed in Virginia. Based on these false representations, clients paid fees ranging from $2,500 to $25,000 to modify the terms of their mortgages. Shmuckler was indicted and is awaiting trial, currently scheduled for early 2012. This case was jointly investigated by the FBI, FDIC-OIG, and SIGTARP.

**Carl Cole; David Crisp (Sacramento):** In January 2011, a 56-count indictment was returned against 10 subjects for their roles in a large-scale loan origination scheme. The scheme included approximately 140 fraudulent mortgage transactions on 108 properties with loans totaling $142 million. This investigation was initiated in December 2006. Carl Cole and David Crisp, partners in Crisp and Cole Real Estate (CCRE), utilized CCRE to orchestrate an extensive loan origination mortgage fraud scheme. The scheme involved several mortgage brokers, appraisers, realtors, loan officers, certified public accountants, bank/financial institution employees, straw buyers, title companies, and builders.

## IV. Mortgage Fraud Schemes and Trends

**Foreclosure Rescue Schemes -** The perpetrators identify homeowners who are in foreclosure or at risk of defaulting on their mortgage loan. The perpetrators then mislead the homeowners into believing they can save their homes by transferring the deed or putting the property in the name of an investor. The perpetrators profit by selling the property to an investor or straw borrower, creating equity using a fraudulent appraisal, and stealing the seller proceeds

or fees paid by the homeowners. The homeowners are sometimes told they can pay rent for at least a year and repurchase the property once their credit has been reestablished. However, the perpetrators fail to make the mortgage payments and usually the property goes into foreclosure.

**Loan Modification Schemes** - Scammers purport to assist homeowners who are delinquent in their mortgage payments and are on the verge of losing their home by offering to renegotiate the terms of the homeowners' loan with the lender. The scammers, however, demand large fees upfront and often negotiate unfavorable terms for the clients, or do not negotiate at all. Usually, the homeowners ultimately lose their homes. This scheme is similar to a foreclosure rescue scam.

**Illegal Property Flipping -** Property is purchased, falsely appraised at a higher value, and then quickly sold. What makes property flipping illegal is the appraisal information is fraudulent. The schemes typically involve one or more of the following: fraudulent appraisals; falsified loan documentation; inflated buyer income; and kickbacks to buyers, investors, property/loan brokers, appraisers, and title company employees.

**Builder Bailout/Condo Conversion** - Builders facing rising inventory and declining demand for newly constructed homes employ bailout schemes to offset losses. Builders find buyers who obtain loans for the properties. The buyers then allow the properties to go into foreclosure. In a condo-conversion scheme, apartment complexes purchased by developers during a housing boom are converted into condos. When the market declines, developers have excess inventory of units. Developers recruit straw buyers with cash-back incentives and inflate the value of the condos to obtain a larger sales price at closing. In addition to failing to disclose the cash-back incentives to the lender, the straw buyers' income and asset information are often inflated in order for them to qualify for properties that they otherwise would be ineligible or unqualified to purchase.

**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.

**Silent Second -** The buyer of a property borrows the down payment from the seller through the issuance of a nondisclosed 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.

**Home Equity Conversion Mortgage (HECM) -** A HECM is a reverse mortgage loan product insured by the Federal Housing Administration to borrowers who are 62 years or older, own their own property (or have a small mortgage balance), occupy the property as their primary residence, and participate in HECM counseling. It provides homeowners access to equity in their homes usually in a lump sum payment. Perpetrators recruit seniors through local churches, investment seminars, and television, radio, billboard, and mailer advertisements. The

scammers then obtain a HECM in the name of the recruited homeowner to convert equity in the homes into cash. The scammers keep the cash and pay a fee to the senior citizen or take the full amount unbeknownst to the senior citizen. No loan payment or repayment is required until the borrower no longer uses the house as a primary residence. In the scheme, the appraisals on the home are vastly inflated and the lender does not detect the fraud until the homeowner dies and the true value of the property is discovered.

**Commercial Real Estate Loans** - Owners of distressed commercial real estate obtain financing by creating bogus leases and using these fake leases to exaggerate the building's profitability, thus inflating their appraisal values using the income method approach. These false leases and appraisals trick lenders into extending loans to the owner. As cash flows are restricted to the borrower, property repairs are neglected. By the time the commercial loans are in default, the lender is oftentimes left with dilapidated and unusable or difficult-to-rent commercial property. Many of the methods of committing mortgage fraud that are found in residential real estate are also present in commercial loan fraud.

**Air Loans -** This is a nonexistent property loan where there is usually no collateral. Air loans involve brokers who invent borrowers and properties, establish accounts for payments, and maintain custodial accounts for escrows. They may establish an office with a bank of telephones, each one used as the fake employer, appraiser, credit agency, etc., to fraudulently deceive creditors who attempt to verify information on loan applications.

For additional information regarding mortgage fraud schemes and trends, please see the FBI Annual Mortgage Fraud Report which can be found at **http://www.fbi.gov/stats-services/publications/mortgage-fraud-2010.**

## Mortgage Fraud Prevention Measures

### Tips to Protect Yourself Against Mortgage Fraud

- Get referrals for real estate and mortgage professionals. Check the licenses of the industry professionals with state, county, or city regulatory agencies.
- 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. If you do not understand, re-read the documents or seek assistance from an attorney or third party who represents your interest.
- Review the title history of the home you are anticipating to purchase 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 personal

information against the information as listed on the loan documents to ensure it is accurate and complete.

- Never sign any loan documents that contain "blanks." This leaves you vulnerable to fraud.
- Check out the tips on the MBA website at **http://www.StopMortgageFraud.com** for additional advice on avoiding mortgage fraud.

## Tips to Protect Yourself Against 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 upfront 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 easy method to relieve your debts.
- Borrowers may end up paying thousands of dollars in fees without the elimination or reduction of any debt.

## Tips to Protect Yourself Against Foreclosure Fraud Schemes

- 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.
- Do not pay advanced fees for promised services.

# FINANCIAL INSTITUTION FRAUD

## I. General Overview

FIF investigations are among the most demanding, difficult, and time-consuming cases undertaken by law enforcement in the area of white collar crime. Other than mortgage fraud, areas of primary investigative interest relative to FIF include insider fraud (embezzlement and misapplication), check fraud, counterfeit negotiable instruments, check kiting, and fraud contributing to the failure of financial institutions.

With the onset of the U.S. housing crisis that began in 2007, as well as the global financial crisis, mortgage fraud became a primary focus of the FIFU. Although resources were shifted to combat mortgage fraud, the FBI continues to address other fraud schemes that impact our financial institutions. FIF investigations related to emerging technologies and computer-related banking are taking on added significance among the nation's financial institutions.

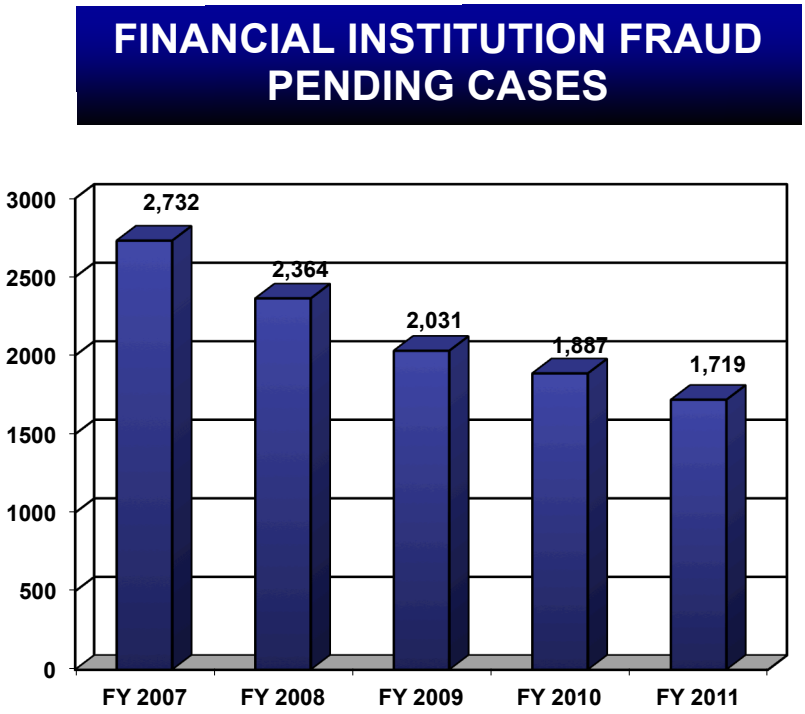
The FBI continues to concentrate its efforts on organized criminal groups involved in FIF. These groups are often involved in the sale and distribution of stolen and counterfeit corporate checks, money orders, payroll checks, credit and debit cards, U.S. Treasury checks, and currency. Furthermore, the groups involved in check and loan fraud schemes are often involved in illegal money laundering activities in an effort to conceal their illegal proceeds. The FBI often utilizes asset forfeiture statutes to seize and forfeit the proceeds of criminal activity.

The FBI, USPIS, and the IRS conduct criminal FIF investigations with the goal of disrupting and dismantling organized fraud rings, as well as addressing individuals who continue to manipulate internal controls either alone or in collusion with others. The FBI strongly supports joint investigations to effectively utilize limited resources while strengthening investigations by tapping into each agency's expertise. Federal agencies work with state and local law enforcement, regulators, and the financial institution industry to combat this crime problem.

The FBI fosters relationships and partnerships within the banking industry to promote FIF awareness. To raise awareness and increase accessibility to investigative personnel, the FBI has designated points of contact with relevant groups including the National Bank Fraud Working Group, local Bank Fraud Working Groups, and SAR Working Groups across the nation. Included among these working groups are federal, state, and local law enforcement partners, regulatory industry representatives, as well as banking industry representatives.

## II. Overall Accomplishments

During FY 2011, cases pursued by the FBI resulted in 521 informations and indictments, and 429 convictions of FIF criminals. The following are notable statistical accomplishments in FY 2011 for FIF: $1.38 billion in restitutions, $116.3 million in fines, and seizures valued at $15.7 million. The chart below reflects pending FIF cases from FY 2007 through FY 2011 as follows: FY 2007 - 2,732 cases; FY 2008 - 2,364 cases; FY 2009 - 2,031 cases; FY 2010 - 1,887 cases; and FY 2011 - 1,719 cases.




## III. Significant Cases

**Anthony Raguz (Cleveland):** On September 27, 2011, Anthony Raguz, the former Chief Operating Officer of the St. Paul Croatian Federal Credit Union (FCU), pleaded guilty to six counts, including bank fraud, money laundering, and bank bribery, for his role in one of the largest credit union failures in American history. Raguz issued more than 1,000 fraudulent loans totaling more than $70 million to over 300 account holders in the Albanian and Croatian communities near Cleveland from 2000 to 2010. He accepted more than $1 million worth of bribes, kickbacks, and gifts in exchange for the fraudulent loans. Raguz is one of 16 people charged for their roles in the credit union's collapse. The failure of St. Paul Croatian FCU resulted in a $170 million loss to the National Credit Union Share Insurance Fund.

**Gary Foster (New York):** Gary Foster, a former vice president in Citigroup's treasury finance department, pleaded guilty on September 6, 2011, to bank fraud stemming from his embezzlement of more than $22 million from Citigroup. Between September 2003 and June

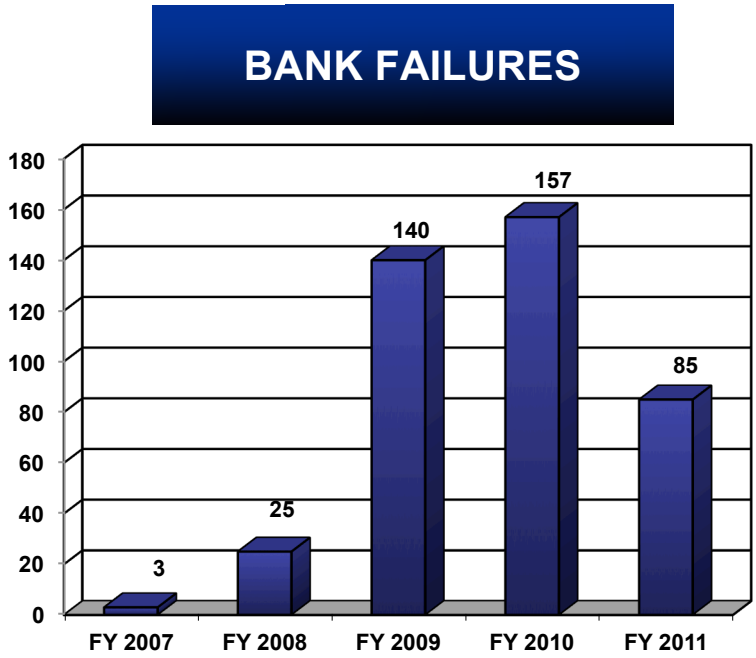
2011, Foster first transferred money from various Citigroup accounts to Citigroup's cash account, then wired the money to his personal bank account at another bank. Foster concealed his thefts by making various false accounting entries to create the appearance that the cash account was in balance and by placing a fraudulent contract or deal number in the reference line of the wire transfer instructions to give the appearance the wire transfers were actually in support of an existing Citigroup contract. Foster used the money to buy real estate and luxury automobiles, including a Ferrari and a Maserati.

**William T. Hernandez (Louisville):** On September 20, 2011, William T. Hernandez was sentenced to 41 months in prison and ordered to pay $453,819 in restitution for embezzling money from elderly customers. Between October 2006 and June 2010, Hernandez, who was an investment banker employed by PNC Investments at the time, transferred money from investment accounts maintained with PNC Investments. Hernandez deposited the money into a PNC account, then issued cashier's checks for his personal benefit and gain. Hernandez pleaded guilty on June 21, 2011, to two counts of bank fraud.

# FINANCIAL INSTITUTION FAILURES

## I. General Overview

The FBI began to track the number of financial institution failure investigations in February 1986. A total of 157 banks failed in 2010, and 85 have failed since January 1, 2011, with the total number reaching 410 closures since 2007. Last year saw the highest number of bank failures since 1992 when 181 institutions closed. By comparison, over 1,000 banks failed between 1987 and 1992, and more than 9,000 failed during the Great Depression, between 1930 and 1933.




In addition, there are currently 865 U.S. banks on the Federal Deposit Insurance Corporation (FDIC) "Problem List" as of June 30, 2011. Problem banks account for about 11 percent of all banking institutions. As of October 2011, there were 7,433 FDIC-insured banking institutions with FDIC-insured deposits of almost $9.8 trillion and assets totaling over $13.6 trillion. Of these institutions, about 4,600 are regulated by the FDIC and the remainder are supervised by the Office of the Comptroller of the Currency and the Federal Reserve. In addition, the National Credit Union Administration is charged with supervising the 7,239 active federally insured credit unions.

The vast majority of the failed banks have closed as a result of market conditions (e.g., devalued properties) associated with the current financial crisis. Their solvency is usually compromised because of unsafe and unsound banking practices and inappropriate risk management tied to heavy concentration of commercial real estate and acquisition, development, and construction loans. The catalyst for the failure has been the economic climate and not criminal activity. Upon closer inspection of the loan portfolios, however, some level of fraud is usually uncovered in many of the loans.

## II. Overall Accomplishments

One of the outcomes of the financial crisis that began in 2007 was the failure of the largest number of U.S. banks since the savings and loan crisis of the 1980s. As a result of the nature of this financial crisis, bank failure investigations have been opened at the FBI under a myriad of classifications, such as mortgage fraud, corporate fraud, and bank fraud. Of the 1,719 pending FIF investigations, only 49 cases, or about 2.85 percent, involve criminal activity related to a failed federally insured financial institution.

## III. Significant Cases

**Donna Shebetich (Pittsburgh):** On October 6, 2010, Donna Shebetich was indicted on five counts of filing false Call Reports to the FDIC. Shebetich, a former vice president, director, and loan officer at Metropolitan Savings Bank, underreported millions of dollars in delinquent mortgages shortly before the Pittsburgh bank failed and its deposits were taken over by another bank. Shebetich filed five false quarterly reports with the FDIC. In the last report filed in November 2006, three months before the bank failed, she listed $0 in delinquent mortgages, when the bank really had more than $7 million in loans at least 30 days overdue. The bank had roughly $15.8 million in assets in that quarter.

**Elexa Manos (Pittsburgh):** On June 6, 2011, Elexa Manos pleaded guilty to one count of bank fraud in connection with a scheme to steal $4 million from the Dwelling House Savings & Loan, a historic African-American financial institution founded in the 1890s, causing it to fail. Beginning in about 2006, Manos stumbled upon and then exploited weaknesses in the internal controls of the savings and loan's Automated Clearing House (ACH) system. Manos and other individuals she recruited, including her son, withdrew funds from 13 savings accounts via ACH debits or withdrawals. The transactions were fraudulent because the accounts did not have sufficient funds available to cover the amounts being withdrawn, causing the bank to use all of its capital reserves to absorb the losses. The funds were used to pay various vendors and creditors, as well as to fund electronic PayPal accounts. Manos was sentenced to 150 months' incarceration and ordered to pay $2.5 million in restitution.

**Robert E. Maloney, Jr. (Atlanta):** On June 22, 2011, Robert E. Maloney, Jr., was indicted in a multimillion-dollar fraud and money laundering conspiracy. This superseding indictment charged Maloney and two former top officers of First City Bank (FCB) of Stockbridge, Georgia, with conspiracy to commit bank fraud, bank fraud, and related crimes in connection with misconduct at FCB in the years before the bank's seizure by state and federal authorities on March 20, 2009. Maloney assisted Mark Connor, the former bank president, and

Clayton Coe, a senior lending officer, with massive insider dealing and fraud that preceded the bank's failure. The dollar loss from the fraudulent activity caused FCB to fail and was a contributing factor in the failure of several other Georgia banks.

# INSURANCE FRAUD

## I. General Overview

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.

The FBI continues to identify the most prevalent schemes and the top echelon criminals defrauding the insurance industry in an effort to reduce insurance fraud. The FBI works closely with the National Association of Insurance Commissioners, the NICB, the 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 nonprofit organization whose mission is to maintain an international presence to address insurance and insurance-related financial crimes on a global basis.

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. Currently, the FBI is focusing a majority of its resources relating to insurance fraud on the following schemes:

**Premium Diversion/Unauthorized Entities** - The most common type of fraud involves insurance agents and brokers diverting policyholder premiums for their own benefit. There are 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) increase the possibility for this type of fraud.

**Insurance-Related Corporate Fraud** - Although corporate fraud is not unique to any particular industry, there have been instances involving insurance companies caught in the web of these schemes. The temptations for fraud within the insurance 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.

**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. Additionally, 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.

**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 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 that 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 United States. This insurance fraud scheme has left injured and deceased victims without workers' compensation coverage to pay their medical bills.

**Disaster Fraud** - When a disaster occurs, there are often individuals who seek to profit via false claims of damages. Additionally, there are also non-insurance related disaster frauds as many organizations and individuals soliciting contributions for the victims of this disaster. Most of the organizations and individuals involved are legitimate; however, there are some who are not. Victims may be approached by unsolicited e-mails asking for donations to a legitimate-sounding organization. The schemer will instruct the victim to send a donation via a money transfer.

Following the 2005 Hurricanes Katrina, Rita and Wilma, billions of dollars in federal disaster relief poured into the gulf coast region. In order to screen, de-conflict and refer reports of fraud to law enforcement, DOJ established the National Center for Disaster Fraud (NCDF) for individuals to report suspected fraud related to any type of disaster relief. The FBI and the NCDF have established a 24-hour hotline that the public can contact in order to report suspected scams and/or fraud associated with disaster relief such as the BP Oil Spill relief effort. The public can report suspicious activity by telephone at (866) 720-5721 or by e-mail at disaster@leo.gov.

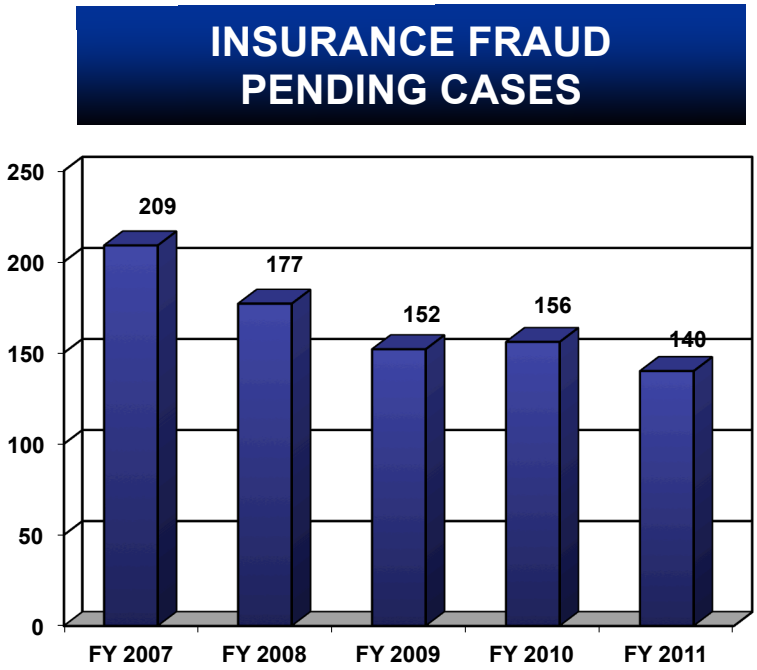
**Staged Auto Accidents** - Perpetrators of staged auto accidents will either stage an accident with coconspirators, or maneuver innocent motorists into accidents. Although the resulting property damage may be small, the perpetrators make large – and illegal – claims for

fake injuries and property damage. This type of fraud results in higher insurance premiums for all drivers. In some cases, innocent victims have been killed or injured in a staged auto accident gone wrong.

**Property Insurance Fraud** - Perpetrators of property insurance fraud seek to obtain payment that is higher than the value of the property damaged or destroyed, or intentionally destroy property that could not be sold. Common examples include arson, scuttling of boats, and the ditching of vehicles in lakes or canals.

## II. Overall Accomplishments

During FY 2011, 140 cases investigated by the FBI resulted in 19 indictments/informations, 13 arrests, and 21 convictions of insurance fraud criminals. In addition, the FBI obtained $87.6 million in restitutions in FY 2011 for insurance fraud. Although the FBI has focused its efforts on higher priority WCC matters, insurance fraud investigations continue to be important and are often addressed utilizing liaison efforts in conjunction with other federal, state, and local law enforcement. The chart below reflects insurance fraud pending cases from FY 2007 through FY 2011 as follows:




## III. Significant Case

**Ronald Allen (Newark):** On July 26, 2011, Ronald Allen was sentenced to 70 months in prison for diverting policyholder premiums for his own benefit. Allen, along with a number of coconspirators, sold insurance liability policies to high-risk business, such as restaurants and bars. Premiums were diverted and legitimate insurance policies

were never issued. A number of businesses that thought they had insurance had claims filed against them. These claims could cost the businesses millions of dollars to cover claims that they thought were covered by the fictitious insurance policies. The aforementioned premium diversion insurance fraud is the most common type of insurance fraud that is reported to the FBI.

# MASS MARKETING FRAUD

## I. General Overview

Mass marketing fraud is a general term for frauds which exploit mass-communication media, such as telemarketing, mass mailings, and the Internet. Since the 1930s, mass marketing has been a widely accepted and exercised practice. Advances in telecommunications and financial services technologies have further served to spur growth in mass marketing, both for legitimate business purposes, as well as for the perpetration of consumer frauds. They share a common theme: the use of false and/or deceptive representations to induce potential victims to make advance fee-type payments to fraud perpetrators. Although there are no comprehensive statistics on the subject, it is estimated mass marketing frauds victimize millions of Americans each year and generate losses in the hundreds of millions of dollars. The following is a brief description of some of the key concepts and schemes associated with the mass marketing/advance fee fraud crime problem.

**Advance Fee Fraud** - This category of fraud encompasses a broad variety of schemes which are designed to induce their victims into remitting upfront payments in exchange for the promise of goods, services, and/or prizes. Some of the most prevalent schemes being encountered are the following:

**Nigerian Letter Fraud** - Victims are contacted regarding substantial sums of money held in foreign accounts and are requested to pay various fees to secure their transfer to the United States, in exchange for a portion of the total proceeds. Alternatively, victims are asked to act as a U.S. agent in securing the release of such funds and are provided with counterfeit instruments which are to be cashed in order to pay any required fees, only to discover they must reimburse their financial institution for cashing a counterfeit instrument. A variation of this fraud involves the use of fraudulent websites, which have been created to resemble website pages of legitimate financial institutions, to enhance the scheme's credibility and swindle greater amounts of money from victims. The victims are directed to open accounts at the fictitious banks' websites into which the perpetrators transfer the victims' funds. Victims cannot withdraw or transfer the funds when they log on to the fictitious bank websites and are prompted to pay additional taxes or fees before the funds can be released. The funds are never released.

**Foreign Lottery/Sweepstakes Fraud** - Victims are informed they have won a substantial prize in a foreign drawing, but must remit payment for various taxes/fees to receive their winnings. Alternatively, victims are provided with counterfeit instruments, representing a

portion of the winnings, which are to be cashed in order to pay the required fees, only to discover they must reimburse their financial institution for cashing a counterfeit instrument.

**Overpayment Fraud** - Victims who have advertised some item for sale are contacted by buyers who remit counterfeit instruments, in excess of the purchase price, for payment. The victims are told to cash the payments, deduct any expenses, and return or forward the excess funds to an individual identified by the buyer, only to discover they must reimburse their financial institution for cashing a counterfeit instrument.

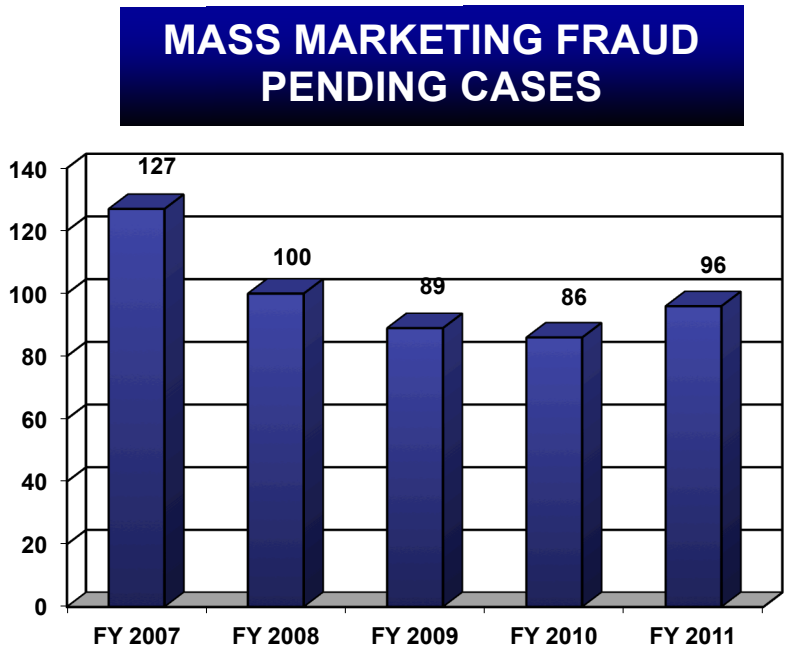
**Recovery/Impersonation Schemes** - Victims are contacted by perpetrators posing as law enforcement officers, government employees, or lawyers to inform victims that the persons responsible for the original fraud schemes have been arrested or successfully sued and their bank accounts have been seized. The victims are told the seized money is going to be returned to the victims, but the victims must first pay fees for processing and administrative services. Recovery pitches often target victims many months or years after the original fraud schemes.

The predominantly transnational nature of the mass marketing fraud crime problem presents significant impediments to effective investigation by any single agency or national jurisdiction. Typically, victims will reside in one or more countries, perpetrators will operate from another, and the financial/money services infrastructure of numerous additional countries are utilized for the rapid movement and laundering of funds. For these reasons, the FBI is uniquely positioned to assist in the investigation of these frauds through its network of Legal Attache (Legat) Offices located in over 60 U.S. embassies around the world. By leveraging its global presence and network of liaison contacts, the FBI has successfully cooperated with other domestic and foreign law enforcement agencies to combat, disrupt, and dismantle international mass marketing fraud groups. The FBI participates in the International Mass Marketing Fraud Working Group (IMMFWG), a multiagency working group established to facilitate the multinational exchange of information and intelligence, the coordination of cross-border operational matters, and the enhancement of public awareness of international mass marketing fraud schemes. The current membership of the IMMFWG consists of law enforcement, regulatory, and consumer protection agencies from seven countries, including Australia, Belgium, Canada, the Netherlands, Nigeria, the United Kingdom, and the United States.

Despite the best interagency enforcement efforts to combat mass marketing fraud, the FBI remains cognizant of the fact the only enduring remedy for this crime problem lies in consumer education and fraud prevention programs. Towards this end, the FBI has not only produced its own mass marketing fraud prevention materials, but coordinates on other public information efforts with the DOJ, FTC, and the USPIS, among others. The FBI also supports a consumer fraud prevention website in conjunction with the USPIS which can be located on the web at: http://www.lookstoogoodtobetrue.gov. Additionally, further information on mass marketing fraud schemes can be found at www.fbi.gov, www.ftc.gov, www.ic3.gov, and www.stopfraud.gov.

## II. Overall Accomplishments

As of the end of FY 2011, the FBI was investigating 96 cases of mass marketing fraud and during FY 2011 recorded multiple indictments and convictions. Although the FBI has focused its efforts on higher priority financial crimes matters, mass marketing fraud investigations continue to be addressed utilizing liaison efforts in conjunction with other federal, state, and local law enforcement agencies and the IMMFWG. The chart below reflects mass marketing fraud pending cases from FY 2007 through FY 2011 as follows:




## III. Significant Cases

**Foreign Lottery/Sweepstakes Fraud (New York):** This investigation centered on the activities of Israel-based telemarketing con men that pitched winnings in an international lottery sweepstakes primarily to elderly American victims. The victims were informed they won the lottery, but first had to send over payment to cover taxes and fees to have the money released and sent to their account. However, there was no lottery and the perpetrators would just keep the funds for personal use and continue to try to solicit victims for additional fees and taxes to release their alleged winnings. A total of nine subjects were charged, and seven of the subjects, all Israeli nationals, were extradited to the United States and sentenced to prison terms that ranged from 33 months to nine years. This is the largest number of Israeli citizens ever extradited to a foreign country in a single case. This investigation was extremely successful in large part due to the FBI's continued use of sophisticated investigative techniques to address

financial crimes and the outstanding cooperation and assistance provided by the Tel Aviv Fraud Division of the Israel National Police. Total victim losses were approximately $2 million.

**Foreign Lottery/Sweepstakes Fraud (Los Angeles):** This investigation centered on the activities of Vancouver, Canada-based telemarketing businesses that pitched European prize bonds to primarily elderly Americans. These companies promised victims that their money would be pooled and used to purchase lottery tickets, that the victims had a very good chance of winning money, or that the victims had actually won a large sum of money. Fraudsters also told victims their money would buy a bond and their investments were guaranteed, meaning they could obtain refunds of their initial investments after a short period of time. However, the victims' money was never used to provide any benefit to victims, and none of the victims ever received any substantial payment from the fraudulent companies. Approximately 4,500 individuals, mostly elderly, were victimized by this scheme. The main subject was sentenced to nine years in prison and ordered to repay victims $4.76 million. This case was investigated by FBI Los Angeles, in conjunction with the USPIS, FTC, and the Royal Canadian Mounted Police.

**Foreign Lottery/Sweepstakes Fraud (Los Angeles):** This investigation centered on the activities of several lottery companies based in London, England. Using phone calls, letters and emails, subjects contacted potential victims, telling them they had won a lottery prize. However, to collect the winnings, victims had to call telemarketers in Spain or England, who told the victims they had to pay taxes or other fees to receive prizes that never materialized. Approximately 52 victims, primarily elderly, were defrauded out of more than $2.7 million. Victims were from around the world, including the United States and the United Arab Emirates. The main subject was sentenced to 14 years in prison. This case was investigated by FBI Los Angeles and the Metropolitan Police Service in London.

## Tips to Protect Yourself Against Mass Marketing Fraud

**Things you should do:**

- Insist on learning the full name, address, and contact information for any company soliciting your business, personal information, or assistance.
- Insist that all solicitors send materials to you in writing so that you are able to study the full details of the offer, as well as any guarantees, and/or refund policies.
- Research all solicitors through the Better Business Bureau, state Attorney General's Office, and/or consumer protection service in the state or city where the company is located.
- Prior to making any significant financial decisions, consult a family member, friend, your attorney, accountant, and/or other trusted advisor for an objective opinion.
- To stop receiving telephone solicitations, instruct solicitors to delete your contact information from all call lists and register with the FTC's "Do Not Call" Registry.
- Report suspicious telemarketing calls, mail solicitations, or advertisements to the FTC at 1-877-FTC-HELP or online at http://www.ftc.gov.

**Things you should NOT do:**

- Do not make any payments to either secure a prize or improve your chances of winning a prize.
- Do not be intimidated into making hasty financial decisions by high-pressure sales tactics.
- Do not provide anyone with your sensitive personal or financial information unless:
  a) it is to an entity whose legitimacy is personally known to you, and
  b) you personally initiated the contact with the entity.
- Do not send funds via wire or electronic money transfer services unless:
  a) it is to an entity whose legitimacy is personally known to you, and
  b) you personally initiated the contact with the entity.
- Do not deposit checks and wire back any fees using the check proceeds until the checks have fully cleared. It is common for a fraudster to send a check to victims with a requirement that a portion of the check be returned to the fraudster (e.g. wire back taxes on winnings using part of the check or wiring back excess amount received for something you were selling).
- Do not be lured by offers that are simply too good to be true...they almost certainly are.

## 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 field offices employ the money laundering violation in all investigations, where appropriate, to disrupt and/or dismantle criminal enterprises. The asset forfeiture and money laundering process identifies, targets, disrupts, and dismantles criminal and terrorist organization and individuals engaged in fraud schemes which target our nation's financial infrastructure.

The implementation of the asset forfeiture process to criminal investigations provides law enforcement with the opportunity to deprive wrongdoers of the proceeds of their crimes, recover property that may be used to compensate victims, and deter future criminal activity. The asset forfeiture process can destroy the financial infrastructure of criminal enterprises, return funds to victims of large-scale fraud, and share forfeited property with state and local law enforcement agencies.

The AF Program and the ML Program provide support to all FBI investigative programs, to include International and Domestic Terrorism.

## MONEY LAUNDERING

The DOJ 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, thereby giving criminals unwarranted economic power."

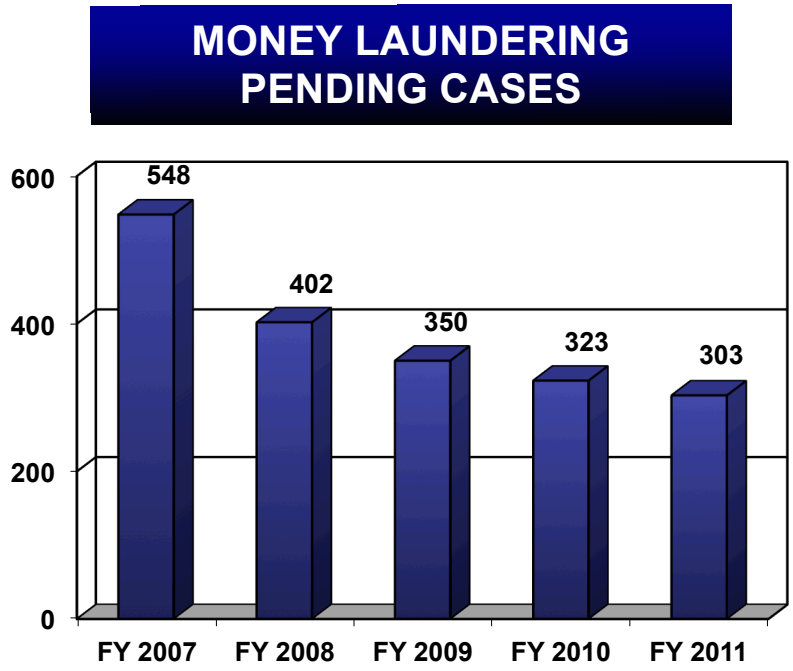
The FBI maintains a proactive approach when investigating money laundering. After identifying a Specified Unlawful Activity that generates illicit proceeds, a parallel financial investigation is conducted in order to locate the proceeds and prove their connection to the underlying crime.

## ASSET FORFEITURE

The FBI's AF Program is one of the most successful in all of law enforcement. In the 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 2011, 303 cases investigated by the FBI resulted in 37 indictments and 45 convictions of Money Laundering Fraud criminals. For FY 2011, the following Money Laundering accomplishments were achieved for the WCCP: $18.4 million in restitutions, $809,414 in recoveries, and $983,536 in fines. The chart below reflects pending Money Laundering cases from FY 2007 through FY 2011 as follows: FY 2007 - 548 cases; FY 2008 - 402 cases; FY 2009 - 350 cases; FY 2010 - 323 cases; and FY 2011 - 303 cases.




**III. Significant Cases**

**Barclays (New York):** On August 16, 2010, Barclays Bank entered into a Deferred Prosecution Agreement waiving indictment and the filing of a two-count Criminal Information charging violations of Title 50, United States Code (USC), Section 1705, the International Emergency Economic Powers Act (IEEPA) and Title 50, USC, Section 5 & 16, Trading With the Enemy Act (TWEA). Under IEEPA and TWEA, it is a crime to willfully violate, or attempt to violate, any regulation issued under the act, including those related to Cuba, Iran, Libya, Sudan, and Burma. The IEEPA and TWEA regulations are administered by the Office of Foreign Assets Control (OFAC). This investigation resulted in the forfeiture of $298 million.

**Credit Suisse (New York):** On December 16, 2009, Credit Suisse entered into a Deferred Prosecution Agreement waiving indictment and the filing of a one-count Criminal Information in violation of Title 50, USC, Section 1705, the IEEPA. The violations relate to transactions Credit Suisse illegally conducted on behalf of customers from Iran, Sudan, and other countries sanctioned in programs administered by the Department of the Treasury's OFAC. This investigation resulted in the forfeiture of $536 million, which was the largest forfeiture ever received for this type of violation.

# FORENSIC ACCOUNTANT PROGRAM

## I. General Overview

The Forensic Accountant Unit (FAU) was established in March 2009 to support all FBI investigative matters requiring a forensic financial investigation. The FAU provides oversight of the Forensic Accountant (FoA) and Financial Analyst (FA) Programs, ensuring that the FBI's financial investigative needs and priorities are continuously addressed. Key to the FAU's mission is developing, managing, and enhancing the FoA and FA Programs, to ensure that FBI financial investigative matters are expedited with the high-level of expertise required in an increasingly complex global financial system.

The Forensic Accountant Program (FAP) is the culmination of years of effort to advance and professionalize the FBI's financial investigative capabilities. The FoA position was developed to attract and retain top-tier accounting professionals, who possess the ability to conduct complex, thorough forensic financial investigations. The FBI's FoAs are expected to testify as expert witnesses in judicial proceedings after completing the financial investigative portion of complex investigations.

The mission of the FAU is to support all FBI investigative matters requiring a forensic financial investigation and to ensure the FBI's financial investigative priorities are continually addressed. The FAU seeks to provide the highest caliber of financial investigative work product and support as well as contributing to the FBI's Intelligence Cycle. The FAU continues to develop and implement a rigorous training curriculum and is collaborating with an array of public and private organizations in an effort to cultivate a workforce that provides superior results both in the field offices and at FBIHQ.

## II. Initiatives

### Forensic Accountant Support Team

The Forensic Accountant Support Team (FAST) is stationed within the FAU enabling the FBI to quickly respond to significant, high-profile investigations and augment field office resources to notably advance an investigation. This professional support workforce is an asset to all FBI investigative programs and enables the FBI to more efficiently and effectively conduct complex investigations requiring a thorough forensic financial review. The seven members of the FAST have worked a number of priority investigations during FY 2011 across a variety of investigative matters.

**Forensic Accountant Core Training Session Training Course**

The Forensic Accountant Core Training Session (FACTS) is a rigorous, comprehensive introductory program of instruction designed to increase an FoA's proficiency in the critical areas necessary to conduct a financial investigation. This extensive course develops the FoA's aptitude and knowledge in handling a financial investigation according to pertinent rules and regulations across a wide variety of subject matters. The material covered focuses primarily on providing an overview of FBI programs and systems, financial investigative topics and techniques, resources available to develop an investigation, legal training, and expert witness-testifying techniques. During FY 2011, the FAU held three courses with a total of 128 graduates.

**BankScan Initiative**

BankScan is an in-house created software application which translates physical bank and credit card statements into an electronic medium, thus dramatically decreasing the time-consuming data-entry process. In FY 2011, the FAU provided BankScan training to three FACTS classes, three field offices, and the Terrorism Financing Operations Section at FBI Headquarters. Each field office was supplied with the necessary software and equipment to implement the BankScan Project. Since its implementation, the FBI has benefited through an exponential increase in financial investigative efficiency and productivity. Through 3Q FY 2011, an estimated 4,270 days (11.7 years) of time was saved by using BankScan.

**Electronic Subpoena Production**

The Electronic Subpoena Production initiative represents a joint undertaking of the FBI's CID, DOJ's Criminal Division Fraud Section, and the IRS. Electronic Subpoena Production requires financial institutions to digitally produce account data stored electronically by relying on existing Rule 17 of the Federal Rules of Criminal Procedure and the updated Federal Reserve Regulation S (effective January 1, 2010). When used in conjunction with BankScan, the introduction of this new process will substantially increase the efficiency and effectiveness of FBI forensic financial investigations.

**Financial Analyst Conversion**

In FY 2011, the FAU began the second phase of the selective conversion process to transition qualified FAs to the FAP to provide the FBI's investigative programs with the highest caliber of financial investigative work product and support. This effort ensures only those individuals satisfying the FoA requirements convert to the FAP. The second phase of the conversion will be completed during the early part of FY 2012.

**Financial Investigative Report**

The FAU deployed the Financial Investigative Report (FIR) template in FY 2011. The purpose of the FIR is to provide FAs and FoAs a standardized organizational tool that consistently presents financial investigative analysis, notes, and details to case Agents (CAs) and

Assistant U.S. Attorneys (AUSAs). The intended result is to create high-quality, uniform reporting, that meets or exceeds the standards set by the CA, AUSA, and the FAP.

## III. Significant Cases

The FAP provided substantial support to the following major cases:

**Fair Finance**: Timothy Durham, James Cochran, and Rick Snow were indicted and charged with wire fraud, securities fraud, and conspiracy to commit securities fraud for allegedly committing a scheme to defraud the investors of Fair Finance. Fair Finance was a privately-held niche lender that specialized in account receivables management and financing consumer installment sales contracts. It is alleged in the indictment that over the last several years, Durham, Cochran, and Snow used Fair Finance investor money to finance other business operations and lifestyle expenditures, unbeknownst to investors. There are over 5,000 victim-investors totaling approximately $200 million in loss. Trial is scheduled for June 2012.

**Galleon Group:** Raj Rajaratnam was recently found guilty by a jury in Manhattan federal court of conspiracy and securities fraud crimes stemming from his involvement in the largest hedge fund insider trading scheme in history. Rajaratnam was the Managing Member of Galleon Management, LLC ("Galleon"), the General Partner of Galleon Management, L.P., and a portfolio manager for Galleon Technology Offshore, Ltd., and certain accounts of Galleon Diversified Fund, Ltd. He was convicted on all 14 counts after an eight-week trial and sentenced to 11 years' incarceration.

**American Therapeutic Corporation (ATC)**: Lawrence Duran, Marianella Valera, and others pled guilty for their roles in a scheme to submit more than $200 million of fraudulent claims to Medicare. The scheme was orchestrated by the above owners and operators of American Therapeutic Corporation (ATC); its management company, Medlink Professional Management Group Inc.; and the American Sleep Institute (ASI). ATC's owners and operators paid kickbacks to owners and operators of assisted living facilities and halfway houses and to patient brokers in exchange for delivering ineligible patients to ATC and ASI. Throughout the course of the ATC and ASI conspiracy, millions of dollars in kickbacks were paid in exchange for Medicare beneficiaries who did not qualify for partial hospitalization program services. Lawrence Duran was sentenced to 50 years in prison for his role in the Medicare fraud scheme, and ordered to pay more than $87 million in restitution, jointly and severally with the co-defendants. Duran's sentence is the longest prison sentence ever imposed in a Medicare Fraud Strike Force case. Marianella Valera was sentenced to 35 years in prison and ordered to pay restitution. Margarita Acevedo, a cooperating witness, was sentenced to 7 ½ years in prison and $72.7 million in restitution. Alan Gumer, MD, Adrianna Mejia, James Edwards, Joseph Valdes, and Nelson Fernandez also pled guilty for their role in the fraud scheme, but have yet to be sentenced. Sentencing for these individuals is scheduled for January 2012.

# FINANCIAL INTELLIGENCE CENTER

## I. General Overview

The Financial Intelligence Center (FIC) is a proactive data exploitation unit, within the FCS, created in September 2009. It is staffed with a cadre of Intelligence Analysts (IA) and Staff Operations Specialists (SOS). The FIC's mission is to provide tactical analysis of financial intelligence datasets and databases by using evolving technology and data exploitation techniques, identify potential criminal enterprises and enhance investigations. Additionally, the FIC has established liaison relationships with other government and regulatory agencies to identify additional data sources to disrupt and dismantle criminal enterprises and others and increase information sharing. The FIC supports the following WCC subprograms:

- Financial Institution Fraud (including mortgage fraud)
- Securities/Commodities Fraud
- Public Corruption
- Fraud Against Government
- Health Care Fraud
- Money Laundering and other crimes

The FIC reviews large datasets to identify potential new targets for investigation (see examples below). Once a potential target is identified, the FIC conducts research using various internal databases and a myriad of external databases, such as Lexis Nexis, Dun and Bradstreet, CLEAR, and Public Access to Court Electronic Records; and data provided by other agencies including the SEC, HHS, FINRA, and the DOJ. The information is then organized using Excel spreadsheets and link chart analyses to "connect the dots" of all the key players. The results of the research and analysis are then summarized and referred to the appropriate field office in the form of a targeting package for their discretion in opening an investigation.

## II. Initiatives

### Securities and Futures SAR Review Project

Analysts who support the Securities/Commodities Fraud program review Securities and Futures SARs using defined parameters to identify potential subjects. They then perform preliminary research to determine if the subjects are valid targets to disseminate to the appropriate FBI field office.

**Public Corruption Economic Stimulus Project**

Analysts who support the Public Corruption and Fraud Against the Government programs research the American Recovery and Reinvestment Act funding distribution to identify vulnerabilities for fraud and prepare targeting packages to disseminate to the appropriate FBI field offices for review and potential case initiation.

**Health Care Fraud Prevention and Enforcement Action Team Project**

Analysts who support the HCF program work with HHS-OIG in collaborative data sharing to identify providers of medical equipment and services engaged in HCF. The FIC performs a detailed analysis of the identified providers and formulates a targeting package that is presented to the applicable field office for review and potential case initiation.

**Health Care Fraud SAR Review Project**

Analysts who support the HCF program review SARS to identify physicians engaged in HCF. The FIC performs a detailed analysis of the potential physicians and formulates a targeting package that is presented to the applicable field office for review and potential case initiation.

**Commercial Real Estate Loan SAR Project**

Analysts who support the FIF subprogram review SARs that reference commercial real estate loans to identify potential targets. After further research, targeting packages are disseminated to the appropriate FBI field offices for review and potential case initiation.

**FDIC Referrals Initiative**

Analysts who support the FIF subprogram, in conjunction with the FIFU, conduct reviews of the FDIC's failed loans issued by various lending institutions to identify current indicators of potential fraudulent activity. The data collected from the loan files is compared to various databases to identify subjects worthy of targeting packages. Once the targeting packages are prepared, they are presented to the applicable field offices for review and potential case initiation.

**Money Laundering National SAR Review Project**

Analysts who support the ML program use this initiative, sponsored by the DOJ, to target money laundering activity with an international nexus. Analysts utilize multiagency resources to review SARs that have the potential for case initiation. The FIC performs a detailed analysis of the potential cases and formulates a targeting package that is presented to the applicable field office for review and potential case initiation.

## Acronyms

| | |
|---|---|
| AF/MLU | Asset Forfeiture/Money Laundering Unit |
| AMA | Agape Merchant Advance, LLC |
| AUSA | Assistant United States Attorney |
| CA | Case Agent |
| CAIF | Coalition Against Insurance Fraud |
| CFTC | Commodities Futures Trading Commission |
| CID | Criminal Investigative Division |
| CMHC | Community Medical Health Center |
| CMS | Centers for Medicare and Medicaid Services |
| DME | Durable Medical Equipment |
| DOJ | Department of Justice |
| DPA | Deferred Prosecution Agreement |
| EBRI | Electronic Bank Records Initiative |
| ECU | Economic Crimes Unit |
| FA | Financial Analyst |
| FACTS | Forensic Accountant Core Training Session |
| FAP | Forensic Accountant Program |
| FAST | Forensic Accountant Support Team |
| FAU | Forensic Accountant Unit |
| FBI | Federal Bureau of Investigation |
| FCB | First City Bank |
| FCS | Financial Crimes Section |
| FDIC | Federal Deposit Insurance Corporation |
| FDA | Food and Drug Administration |
| FFETF | Financial Fraud Enforcement Task Force |
| FIC | Financial Intelligence Center |
| FIF | Financial Institution Fraud |
| FIFU | Financial Institution Fraud Unit |
| FINRA | Financial Industry Regulation Authority |
| FIR | Financial Investigative Report |
| FoA | Forensic Accountant |
| FOREX | Foreign Currency Exchange |
| FSP | Forfeiture Support Project |
| FTC | Federal Trade Commission |
| FY | Fiscal Year |
| GDP | Gross Domestic Product |
| GSK | Glaxosmithkline |
| HCF | Health Care Fraud |
| HCFU | Health Care Fraud Unit |
| HECM | Home Equity Conversion Mortgage |
| HHS-OIG | Health and Human Services-Office of Inspector General |
| IA | Intelligence Analyst |
| IEEPA | International Emergency Economic Powers Act |
| IMMFWG | International Mass Marketing Fraud Working Group |

| | |
|---|---|
| IRS | Internal Revenue Service |
| LEGAT | Legal Attache |
| MBA | Mortgage Bankers Association |
| ML | Money Laundering |
| NCDF | National Center for Disaster Fraud |
| NHCAA | National Health Care Anti-Fraud Association |
| NICB | National Insurance Crime Bureau |
| OBT | Operation Broken Trust |
| OFAC | Office of Foreign Assets Control |
| OIG | Office of Inspector General |
| PEO | Professional Employer Organization |
| SAR | Suspicious Activity Reports |
| SEC | Securities and Exchange Commission |
| SIGTARP | Special Inspector General for the Trouble Asset Relief Program |
| SOS | Staff Operations Specialist |
| TBW | Taylor, Bean & Whitaker |
| TWEA | Trading With the Enemy Act |
| USAO | U.S. Attorney's Office |
| USPIS | U.S. Postal Inspection Service |
| WCC | White Collar Crime |
| WCCP | White Collar Crime Program |