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

# 2011 The FBI Story


An FBI agent surveys the landscape near Farmington, New Mexico, where he works with tribal and other law enforcement partners to help protect the residents of Native American lands.

# 2011 The FBI Story

**The FBI's Behavioral Analysis Units' (BAUs) Supervisory Special Agent Mark Hilts and his colleague, Supervisory Special Agent Susan Kossler, work in an office of the National Center for the Analysis of Violent Crime (NCAVC) in Virginia in April 2011. The NCAVC and its BAUs provide operational, behavioral, and analytical support to federal, state, local, and international law enforcement and intelligence agencies investigating unusual or repetitive violent crimes, terrorism, cyber crime, threats, and significant non-violent crimes.**

**A Message from FBI Director Robert S. Mueller, III**

For the FBI and its partners, much has changed in the last decade. The terror attacks of 9/11 shifted the focus of national security, making prevention our collective mandate. Remarkable technological change also gave rise to online scams and cyber attacks. Gangs grew in size and strength, proliferating crime in some communities; and greed and corruption affected many Americans, along with banking and other institutions.

The FBI, for its part, has emerged 10 years later a changed organization. More than ever, we are intelligence-driven and threat-focused, business-like in our operations and strategic in our use of resources. Our workforce has grown increasingly analytic and technologically savvy. We work more closely now than ever with our partners—not only across the country, but as a result of the growing globalization of crime and terror, across the world.

You can get a telling glimpse into the FBI of today in this latest edition of *The FBI Story*, our annual collection of news and feature articles from the Bureau's public website. You can read a series of stories on our unprecedented efforts in the war zone of Afghanistan, where we have worked alongside the U.S. military and other partners to gather intelligence, conduct investigations, and mentor Afghan law enforcement. You can get an inside look at our growing cadre of intelligence analysts—how they operate and contribute daily to the FBI's mission. You can also get a glimpse into how we are addressing emerging scams like ATM skimming and enlisting the public's help in new ways to solve cold cases.

Many of the year's most notable accomplishments are chronicled here as well—major cyber operations, large-scale health care fraud and gang takedowns, and historic Mafia busts. And most notably, in less than two months, two of the FBI's Ten Most Wanted Fugitives were removed from the list. On May 1, Osama bin Laden was killed by U.S. forces, not only closing a chapter in the 9/11 terror attacks but yielding valuable new intelligence in the global effort to end violent extremism. And on June 23, notorious Boston mobster James 'Whitey' Bulger was captured by FBI agents in California following a far-reaching public information campaign.

Thank you for your support of the FBI. I hope you enjoy reading this publication.

**Director Mueller speaks at the Pima County Sheriff's Office in Tucson, Arizona on January 9, 2011 on the investigation into the shooting of U.S. Representative Gabrielle Giffords and others a day earlier. AP Photo/Matt York.**

# Organized Retail Theft

## A $30 Billion-a-Year Industry

It's a telling case: a few years ago, members of two criminal organizations in California were charged for their role in a large-scale fencing operation to buy and sell over-the-counter health and beauty products—as well as other items like camera film, batteries, and infant formula—that had been stolen from major retail chain stores. The merchandise was then passed off to crooked out-of-state wholesale distributors, who just sold it back to unsuspecting retailers.

**Industry experts say organized retail crimes like these cost the U.S. about $30 billion a year.** While that estimate includes other crimes like credit card fraud, gift card fraud, and price tag switching, the FBI's Organized Retail Theft program—according to Special Agent Eric Ives of our Violent Crimes/Major Offenders Unit in Washington, D.C.—"specifically focuses on the most significant retail theft cases involving the interstate transportation of stolen property." Organized retail theft, says Ives, is a "gateway crime that often leads us to major crime rings that use the illicit proceeds to fund other crimes—such as organized crime activities, health care fraud, money laundering, and potentially even terrorism."

**Targets and thieves.** The stores targeted for theft run the gamut—from grocery and major department stores to drug stores and specialty shops. The organizations responsible for much of this crime include South American theft groups, Mexican criminal groups, Cuban criminal groups from South Florida, and Asian street gangs from California.

**Fighting back.** According to Ives, the FBI uses many of the same investigative techniques against organized retail theft groups that we do against any criminal enterprise or terror network, especially undercover operations. Organized retail theft cases also present some valuable opportunities for us to enlist confidential human sources—the best sources of intelligence information—in order to dismantle entire operations. We recruit from the ranks of those who steal the merchandise (to a lesser degree) and mid-level fences and individuals higher up in the chain of command (to a greater degree).

**Importzance of collaboration.** We don't do it alone, though. We partner with law enforcement at the federal, state, and local levels, sharing intelligence and working together operationally on seven major theft task forces

located in five cities around the country—Miami, El Paso, Memphis, New York, and Chicago.

We also work closely with the retail industry. Most recently, we assisted in the development of the non-profit **Law Enforcement Retail Partnership Network** (or LERPnet), a secure national database used by retailers to report and share with one another incidents of retail theft and other serious retail crimes. The database, which has helped reveal patterns of organized theft, is now available to law enforcement agencies around the country.

**Overall impact of organized retail theft.** For one thing, it means higher prices for American consumers and less sales tax revenue for state and local governments. There is also a health and safety aspect—in many cases, stolen food products, pharmaceuticals, and other consumables aren't maintained under proper conditions or labeled properly, so when they do finally make their way back to unsuspecting consumers, they may be ineffective or may even make people sick.

All good reasons for the FBI and its partners to continue their collective fight against organized retail theft.

Left: An early photo of the U.S. Embassy building in Paris.

# Legal Attaché Paris

## Then and Now

It took a war to bring the FBI to Paris.

Sixty-seven years ago, in 1944, two FBI agents reported to Colonel Gordon Sheen in France at SHAEF, the Supreme Headquarters Allied Expeditionary Force. Their mission: to get access, at war's end, to captured spies, spy documents, and other source material that might assist U.S. investigations of domestic treason, espionage, and subversive activities. Special Agent Freddy Ayer and Special Agent Don Daughters hit the ground running, "liberating" the apartment that had belonged to the counselor of the German Embassy for a place to stay in post-war Paris, then setting up shop at 15 avenue Mozart, 16th arrondissement.

**It wasn't long before the value of an FBI presence was recognized.** At the request of U.S. Ambassador Jefferson Caffrey, a legal attaché office was established at the U.S. Embassy in Paris on July 16, 1945. Special Agent Horton Telford was appointed the first "legat" and moved into space on the mezzanine floor of the current embassy on the Place Concorde. He was responsible for "maintaining contact, for mutual cooperation purposes, with all sections of the French Police, the International Criminal Police Commission, and the British Intelligence Service."

Consider the Dawson case of that era. Francis Washington Dawson was an American citizen and former employee of the U.S. Embassy who was arrested by French police in Paris following the discovery of incriminating documents in an abandoned German staff car that implicated Dawson in acts of treason against the United States. The U.S. Embassy, newly reopened, asked the FBI to get the facts of the case. Our agents jumped on it, securing the complete story from French police, who also gave them access to Dawson for a direct interrogation.

After discussing the results with Ambassador Caffrey, the case was concluded to the satisfaction of all concerned.

**And so began the friendships and cooperative relationships between the FBI and French law enforcement and intelligence services that flourish to this day.**

Today, Legat Paris is staffed with a French-speaking legat, three assistant legats, a linguist, and two office administrators. The mission hasn't changed all that much—in the words of Assistant Director for International Operations Joe Demarest, the goal is "fostering strategic partnerships with foreign law enforcement, intelligence, and security services as well as other FBI divisions and other government agencies by sharing knowledge, experience, capabilities, and exploring joint operational opportunities." But if the mission hasn't changed, the cases sure have.

Anyone who pays attention to the news could guess that bilateral cooperation with our French colleagues on terrorist investigations would be a top priority—and it is, making up some 75 percent of the office caseload and involving some of the most complex and far ranging terrorist threats in the world today. But major work is also done in areas as diverse as: counterintelligence and weapons of mass destruction; cyber crime, including child pornography and computer intrusions; transnational organized crime; white-collar crime; and fugitives and violent crime.

Looks a lot like the FBI's top priorities, doesn't it? And the investigations can be deliciously high-tech.

Take, for example, Hacker Croll. In 2009, Twitter.com realized someone had hacked into its admin server, downloaded confidential documents, and viewed the individual Twitter account profiles of Barak Obama, Britney Spears, Lindsay Lohan, and Lily Allen, among others. Alerted, the FBI in San Francisco opened an investigation and soon located the hacker—who was sitting just outside Clermont-Ferrand, a beautiful city in central France.

Legat Paris knew just what to do: it contacted *L'Office Central de Lutte Contre la Criminalite Liee aux Technologies de L'Information et de la Communication* of France's Judicial Police. After close consultations, the Judicial Police finalized plans for the arrest—and invited the FBI to accompany the arresting team and to participate in interviews. Twenty-five-year-old Francois Cousteix was arrested on March 23, 2010. He was tried in June, found guilty, and sentenced to prison. C'est la vie! But it never would have happened without the strong and spirited assistance of the French Judicial Police.

# Keeping Kids Safe Online

## FBI Program Offered in Schools

Recent studies show that one in seven youngsters has experienced unwanted sexual solicitations online. One in three has been exposed to unwanted sexual material online. One in 11 has been harassed or bullied online.

And as we all know, these are only some of the dangers that our kids face while surfing the Internet. How can we simultaneously protect them from these threats and enable them to take advantage of the positive things the web has to offer?

In addition to investigating online crimes targeting children, the FBI works to educate kids and their parents about the Internet, sometimes sending cyber agents to visit schools as well as posting useful resources on our public website. We also offer our Safe Online Surfing program to schools to help students understand how to recognize, report, and avoid online dangers.

**How it all started.** The Safe Online Surfing (SOS) program began in our Miami office six years ago, when Special Agent Jim Lewis from one of our cyber squads—who saw first-hand how easily kids could be victimized online—approached a co-worker, Community Outreach Specialist Jeff Green, about his desire to share information about Internet safety with school students.

An online Internet safety program was created that also tested students on what they learned. About 400 South Florida students took part initially, and according to Green, feedback from students and teachers was positive.

Said Green, "Kids are surfing the Internet anyway, so we were just using a vehicle they were comfortable with."

**Over the years**, other FBI field offices began offering the SOS program with the help of their community outreach specialists. By October 2010, our Cyber Division at FBI Headquarters—which manages our Innocent Images National Initiative, focused on online child predators—took the SOS program under its wing and made it a national one. Today, more than 90,000 children in 41 states have completed it.

**How it works.** At each grade level, third through eighth, students read about Internet safety and cyber citizenship and take timed post-quizzes to demonstrate what they've learned. The program also promotes a fun competition:


schools with the highest scoring students in the nation are awarded the FBI-SOS Trophy.

Topics covered in the program run the cyber gamut: depending on the age of the students, they might learn about password security, cyberbullying, virus protection, copyright issues, online predators, e-mail, chat rooms, social networking sites, when to talk to parents or teachers about a threat, and appropriate uses of cell phones and gaming devices.

Of the SOS program, Cyber Division Assistant Director Gordon Snow said, "The Internet is a powerful resource for our youth, but it also presents opportunities for those who would attempt to do them harm…the Safe Online Surfing program is designed to teach young people what they need to know to avoid falling victim to individuals who want to take advantage of their youth and innocence."

Schools interested in signing up for the Safe Online Surfing program should contact the community outreach specialist in their local FBI office or visit https://sos.fbi.gov/.

Left: Boxes of seized contraband cigarettes in a Mississippi warehouse.

# Operation Secondhand Smoke

## Cigarette Case Yields Unexpected Results

When the smoke cleared from Major Case 253, a network of schemers trafficking in contraband cigarettes was dismantled, a Mississippi police department earned a new headquarters, and the FBI gained one more partner in the fight against terrorism.

**Those three things might not seem related, but then again, Operation Secondhand Smoke is no ordinary case.** It began—as many investigations do—when a person of interest in a criminal matter offered information about a larger criminal enterprise, a massive fraud in the cigarette industry.

Working with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Tupelo Police Department, and the Marshall County Sheriff's Office in Mississippi, we began an undercover investigation into a nationwide network of retailers, wholesalers, distributors, importers, and manufacturers who were avoiding cigarette taxes to make millions of dollars in profits.

"The amount of criminal activity in this case to avoid taxes was just phenomenal," said Special Agent Carl Cuneo, one of the case supervisors based in our Oxford, Mississippi Resident Agency.

**In the tobacco industry, the crime is known as "diverting," and it applies to those who scheme to avoid the various federal and state taxes levied on cigarette sales.** Operation Secondhand Smoke involved the so-called fourth-tier market—not well-known cigarette brands, but off-labels such as those manufactured in Armenia.

Taxes represent the majority of the total retail cost of a pack or carton of cigarettes. By illegally avoiding those taxes—through schemes including hiding shipments from auditors and regulators and creating false invoices, bank, and tax records—the crooks pocketed the tax money they should have paid when the cigarettes were sold.

"Every time you avoid a tax, it's pure profit," Cuneo said. "You're talking about as much as a million dollars of profit in just one tractor-trailer of diverted cigarettes." The subjects in the case—six have pled guilty so far to a variety of federal charges—made so much money they bought mansions, vacation properties, boats, and airplanes. "During the execution of just one search warrant," Cuneo said, "we seized $12 million in cash and certificates of deposit. They just had it lying around."

**In one 2009 raid on a warehouse, 28 truckloads of contraband cigarettes were seized worth an estimated $15-$20 million—bad news for the criminals, but very good news for law enforcement.** That's because according to federal law, criminal seizures can be legally forfeited so that cash and property may be returned to victims of crimes or used by law enforcement.

Part of the seized property in Operation Secondhand Smoke was a 100,000-square-foot warehouse located in Tupelo, valued at $1.6 million. Because the Tupelo Police Department played an active role in the investigation from the beginning, that warehouse is in the process of being forfeited to the town, and will become the site of the department's new headquarters. (The Marshall County Sheriff's Department, also part of the investigation from the start, stands to receive as much as $1 million in forfeitures.)

"We're ecstatic about getting a new headquarters," said Tony Carleton, chief of the Tupelo Police Department, which has 115 sworn officers. The city plans to demolish the old warehouse and build a new building.

Based partly on the relationships built between the Tupelo Police Department and the FBI during the Secondhand Smoke investigation, one of the newest members of our Joint Terrorism Task Force (JTTF) in Mississippi is a detective from the police department.

"This case really facilitated the relationship between the FBI and the police department," Cuneo explained. "Everybody worked very hard on this investigation, and the partnerships are continuing to pay off."

# Successes in Gang Enforcement

## From Coast to Coast

Last week, a long-time member and so-called "shot caller" for the Varrio Hawaiian Gardens (VHG) street gang in Los Angeles, California was sentenced to 30 years in prison for helping coordinate the racketeering activities of the gang, including carjackings, kidnappings, and drug trafficking. A sheriff's deputy was also murdered during the VHG's reign.

The week before that, on the other side of the country, the last in a line of 25 gang members named in a racketeering conspiracy in Albany, New York pled guilty in federal court to his involvement in the Original Gangster Killers gang that engaged in criminal activities like drug trafficking, firearms possession, assault, robbery, and attempted murder. He faces a maximum of 40 years in prison.

And in other parts of the country, the FBI and its many law enforcement partners—local, state, and federal—have effectively shut down a number of violent and extremely dangerous street gangs:

- **New Haven, Connecticut:** 35 people were indicted on federal drug and firearms violations after an operation targeting members and associates of several street gangs.
- **Denver, Colorado:** 35 people—many of them gang members—were indicted on charges of trafficking large amounts of cocaine to the Denver area every week.
- **Omaha, Nebraska:** 12 individuals—most gang members—were charged with drug trafficking and firearms violations and are also believed to have been involved in other crimes like assaults, witness intimidation, and robberies.

All told, in the past decade, accomplishments recorded under our violent crime program include 152 undercover operations, 25,498 gang convictions, 1,896 racketeering indictments, and 703 dismantled gangs.

**The reason for these successes?** Our multi-faceted investigative approach using the resources of combined task forces—primarily our 168 Safe Street Task Forces operating around the country—to disrupt the operations of the most violent and dangerous gangs and completely dismantle them, from the top down.


Currently, our task forces include 789 FBI agents and 1,694 task force officers from our partner agencies at the local, state, and federal level working together against the most violent gangs by:

- Identifying past crimes;
- Gathering and analyzing existing intelligence on the gang and its leaders;
- Proactively developing human sources from different segments of the community;
- Developing an investigative plan to exploit a gang's weakness (i.e., its communication network); and
- Using ALL investigative tools available, both overt (i.e., interviews, interrogations, subpoenas, plea agreements) and covert (i.e., physical/electronic surveillance, confidential informants, undercover operations.)

**The overall gang picture.** At least 30,000 violent street gangs, motorcycle gangs, and prison gangs have been identified by law enforcement.

Thirty-nine of those gangs are considered national threats based on their level of criminal activity, violence, and ties to international criminal organizations (like MS-13 and the 18th Street gang). The rest are neighborhood gangs that are often responsible for illegal drug distribution and for a substantial portion of violent crimes within communities.

And while law enforcement has had a recent impact on the threat posed by violent gangs, our efforts to take back the streets of our cities and towns and make them safe once again for innocent citizens will continue. In doing so, we ask for your continued support as well.


Left: Agents looking for a suspect search a house in Brooklyn.

# Mafia Takedown

## Largest Coordinated Arrest in FBI History

Early this morning, FBI agents and partner law enforcement officers began arresting nearly 130 members of the Mafia in New York City and other East Coast cities charged in the largest nationally coordinated organized crime takedown in the Bureau's history.

**Members of New York's infamous Five Families—the Bonanno, Colombo, Gambino, Genovese, and Luchese crime organizations—were rounded up along with members of the New Jersery-based DeCavalcante family and New England Mafia to face charges including murder, drug trafficking, arson, loan sharking, illegal gambling, witness tampering, labor racketeering, and extortion.** In one case involving the International Longshoremen's Association (ILA) at the Ports of New York and New Jersey, the alleged extortion has been going on for years.

More than 30 of the subjects indicted were "made" members of the Mafia, including several high-ranking family members. The arrests, predominantly in New York, are expected to seriously disrupt some of the crime families' operations.

"The notion that today's mob families are more genteel and less violent than in the past is put to lie by the charges contained in the indictments unsealed today," said Janice Fedarcyk, assistant director in charge of our New York Field Office. "Even more of a myth is the notion that the mob is a thing of the past; that La Cosa Nostra is a shadow of its former self."

The Mafia—also known as La Cosa Nostra (LCN)—may have taken on a diminished criminal role in some areas of the country, but in New York, the Five Families are still "extremely strong and viable," said Dave Shafer, an assistant special agent in charge who supervises FBI organized crime investigations in New York.

**Today's operation began before dawn. Some 500 FBI personnel—along with about 200 local, state, and other federal law enforcement officers—took part, including key agencies such as the New York Police Department and the Department of Labor Office of Inspector General.** By 11 a.m., more than 110 of the 127 subjects charged had been taken into custody.

The idea for a nationally coordinated LCN takedown originated at the Department of Justice last summer, said Shafer, a veteran organized crime investigator. "We have done big LCN takedowns before, but never one this big."

Among those charged:

- Luigi Manocchio, 83, the former boss of the New England LCN;
- Andrew Russo, 76, street boss of the Colombo family;
- Benjamin Castellazzo, 73, acting underboss of the Colombo family;
- Richard Fusco, 74, consigliere of the Colombo family;
- Joseph Corozzo, 69, consigliere of the Gambino family; and
- Bartolomeo Vernace, 61, a member of the Gambino family administration.

The LCN operates in many U.S. cities and routinely engages in threats and violence to extort victims, eliminate rivals, and obstruct justice. In the union case involving the ILA, court documents allege that the Genovese family has engaged in a multi-decade conspiracy to influence and control the unions and businesses on the New York-area piers.

"If there's money to be made," said Diego Rodriguez, special agent in charge of the FBI's New York criminal division, "LCN will do it." He noted that today's Mafia has adapted to the times. "They are still involved in gambling and loan sharking, for example, but in the old days the local shoemaker took the betting slips. Now it's offshore online gambling and money laundering. If you investigate LCN in New York," Rodriguez added, "it's a target-rich environment."

# A Case of Florida Fraud

## With a Few Added Twists

Under the sunny skies of southern Florida—specifically, those of Palm Beach County—more than two dozen conspirators spent the past four years stealing away some $10 million from 10 banks in the area through all manner of fraud and corruption.

That's according to a series of federal charges—the latest coming just two weeks ago—filed by prosecutors in the Southern District of Florida following an FBI-led undercover investigation supported by our partners.

**But that's just the beginning of the story.** As it turns out, this was anything but your average white-collar case.

The investigation centered on a scam involving small business loans and lines of credit that worked more like a typical mortgage fraud scheme—loan recipients and/or straw buyers submitting fake documents to generate fast cash.

Key to the swindle were bank insiders who took bribes to push the bogus paperwork through the system. Several of the bankers even became involved in a separate money laundering scheme, agreeing (at the behest of our undercover agent) to set up fake accounts to launder what they thought were illegal drug proceeds, in return for a percentage.

And to top it off, in the process of uprooting these alleged acts investigators uncovered a separate set of crimes—a wave of identity theft targeting the same banks.

**The alleged ringleader of the fraud scheme was the owner of a loan brokerage business called Palm Beach Business Consultants, or PBBC.** The company specialized in fraudulently obtaining loans and lines of credit for clients in need of money fast—for a price, of course, and a steep one, ranging from $12,500 to $25,000 per pop.

According to the charges, the ringleader told clients he had connections with banks that could lend them money even though they may have lacked the income, credit scores, or collateral for legitimate loans or credit lines.

So he had his crooked workers draw up fraudulent loan and credit packages. In most cases, the applications were in the client's name, but occasionally the name of a client's friend or relative with good credit was used instead. Sometimes included on the fraudulent application was the name of an legitimate—but uninvolved—corporation to help seal the deal.


Next, PBBC employees submitted the bogus applications to bank officers on the take—who pocketed from $1,000 to $10,000 for their services. Once the applications were approved and funds distributed, PBBC clients were unable to repay the loans, and the banks were out millions.

So far in the case, 24 individuals have been indicted, including 17 involved in the financial frauds—the ringleader, seven bankers, six PBBC clients, one straw buyer, and two other men already convicted and sentenced.

The other seven conspirators were part of the unrelated identity theft ring that used the names and information of real people to create fictitious drivers' licenses and other phony documents to not only steal from their bank accounts, but also try to obtain bank loans and credit in their names.

**Once again, the case is a wake-up call for those trying to get easy money—whether through shady loans or souped-up returns on investments—without doing their due diligence.** Remember, if it's too good to be true, it most surely is.

# Human Traffickers Indicted

## Massive Case Involves 600 Thai Victims

It seemed pretty straightforward: labor recruiters in Thailand approached impoverished rural farm workers—who made around $1,000 (U.S.) annually—and offered jobs on American farms for higher pay.

Many, hoping to provide a better life for their families, accepted the offer, which was made through an American company called Global Horizons, in the business of recruiting foreign workers to work in the U.S. agricultural industry. But once in the U.S., the Thai workers soon discovered a harsh reality: they worked for little or no pay, and they were held in place with threats and intimidation.

Eventually, their plight became known to law enforcement, and earlier this month, after a multiagency investigation, two additional defendants—accused of being part of the scheme to hold 600 Thai nationals in forced agricultural labor—were indicted in federal court in Honolulu. They joined six individuals who had been indicted last fall.

**Among those indicted?** The CEO of Global Horizons, several Global employees, and two Thai labor recruiters.

The latest indictment alleges a conspiracy among those indicted that began in 2001 and ran until 2007.

**How the scheme worked.**

Thai recruiters allegedly met with rural farm workers, promising them good salaries, lots of hours, decent housing, and an employment contract that guaranteed work for up to three years. All the workers had to do was sign the contract…and pay a "recruitment fee."

The recruitment fees were substantial…anywhere between $9,500 and $21,000. And even though they were given the option of paying a portion of the fee upfront and the rest while working in the U.S., the workers still had to borrow money to pay the smaller amount and up their family's land as collateral.

Meanwhile, back in the U.S., Global Horizons was soliciting client growers—at various agricultural conferences and through mailings—with offers to supply foreign agricultural workers.

**Conditions were tough.**

According to the indictment, once in the U.S., workers found that the work was not as plentiful as they had been led to believe, the hours not as long, and the pay not as good (that is, when they were paid at all).

While working on farms in places like Hawaii and in several other parts of the country, they sometimes lived under brutal circumstances: at one place, workers were crammed into a large shipping container, with no indoor plumbing or air conditioning. Guards were sometimes hired to make sure no one escaped the living quarters. And workers sometimes witnessed threats of violence or experienced it first-hand.

They were made to feel as though they had no way out: workers' passports had been confiscated upon their arrival and they were told if they escaped, they would be arrested and sent back to Thailand, with no way to repay their debts and possibly leaving their families destitute.

**Human trafficking investigations like these are—and will continue to be—a priority under the FBI's Civil Rights Program.** During fiscal year 2010 alone, we opened 126 human trafficking investigations and made 115 arrests, with the assistance of our law enforcement partners often working together on task forces and working groups.

But perhaps more gratifying, we were able to completely dismantle 12 human trafficking organizations. And resulting prosecutions led to $2.7 million in fines and restitution for the victims of human trafficking.

# New and Improved N-DEx

## About to Go Nationwide

Colorado law enforcement working an organized crime case identified a "person of interest" during its investigation but couldn't find a current address or much else on the individual.

So a state trooper searched our Law Enforcement National Data Exchange, or N-DEx, which revealed the subject as a person of interest in an out-of-state drug case worked by a federal agency. The trooper contacted that agency and learned that this individual had been named in other drug-related cases in California.

Based on that information, the trooper began reaching out to other federal, state, and local agencies in California and beyond…and soon discovered that his subject was a member of a violent gang headquartered in Los Angeles that, up until then, wasn't known to be operating in Colorado.

**This process of connecting the dots between seemingly unrelated pieces of criminal data housed in different places is the backbone of N-DEx.** The system enables its law enforcement users to submit certain data to a central repository—located at our Criminal Justice Information Services (CJIS) Division in West Virginia—where it's compared against data already on file from local, state, tribal, and federal agencies to identify links and similarities among persons, places, things, and activities across jurisdictional boundaries.

Until now, N-DEx—accessed through a highly secure Internet site—has only been a viable option for a relatively limited number of agencies.

**Now, we're about to take N-DEx to the next level:** When its final phase is delivered later this month, N-DEx will truly live up to its name…and over time will be available to thousands more law enforcement and criminal justice agencies around the country.

**A quick look at how N-DEx has evolved:**

- 2008: The first phase gave participating agencies basic capabilities, including the ability to create link analysis charts and to search several thousand incident/case report records and arrest data to help determine a person's true identity.


**An example of the N-DEx interface showing a search for records on deceased serial killer Ted Bundy**

- 2009: The second phase supported 100 million searchable records and added the capability to do full-text and geospatial searches. It also enabled users to exchange information with each other and to subscribe to automatic notifications concerning people/cases of interest to them.

**This month's third and final phase** will add probation and parole information to the database, as well as enhancements to some of its existing capabilities. And best of all, the N-DEx interface has been completely redone, giving it the look and feel of a commercial search engine, complete with filters and more streamlined result sets. Now, N-DEx will now be able to support 200 million searchable records, and with future modification, that number can readily increase to two billion records.

**Entering information into N-DEx is easy.** Agencies participating in state or regional information-sharing systems that "feed" N-DEx don't have to do anything. For other agencies, once their data is mapped to N-DEx, contributing data will be as easy as a monthly download and submission. And for smaller agencies without automated record management systems or with fewer records, information can be loaded manually.

**Bottom line:** N-DEx is a powerful investigative tool that will, according to CJIS Assistant Director Dan Roberts, "help keep our communities safer, not only by linking criminal justice data together as never before, but also by enabling investigative partnerships across jurisdictions."

Left: The I-35 Bandit leaps the teller counter during a bank robbery.

# The I-35 Bandit

## Help Us Catch a Serial Bank Robber

A high school teacher was driving down a Texas road when she glanced over to the next lane and saw a man putting on a fake beard while driving. Suspicious, she called 911—just as the man started waving a handgun at her before speeding away. Later that day, a nearby bank was robbed.

**If the robbery was carried out by the I-35 Bandit, as our investigators believe, the car incident was one of only a few mistakes this serial bank robber has made during at least 15 armed heists starting as far back as 2003.**

"What is unique about the I-35 bandit is how lucky he's been to go this long without being caught," said Special Agent Dennis May, bank robbery coordinator in our San Antonio Field Office. May, who has been investigating bank robberies for most of his 19 years in the Bureau, said he has never seen a case quite like this one.

The bandit, so named because his crimes occur mainly in small towns along a major interstate that runs through Texas, is a takeover-style robber. He enters banks with gun drawn and takes everyone hostage while he stuffs cash in a black bag he carries with him.

"He is very quick and usually robs every teller station," May said. Sometimes he pulls up to the front of the bank and leaves the car engine running during the robbery.

He always wears disguises, and they are effective. The fake beard and hair, along with hats, sunglasses, and gloves obscure the robber's face and features. "I am pretty certain that if we saw this guy standing in the parking lot five minutes after the robbery without his disguise on, we'd have no idea it was him," May said.

**That's why we need your help.** "It might take somebody coming forward," May explained, "someone that knows this guy—a cousin, girlfriend, or estranged wife—who will call us and say, 'I think I know who this is.'"

**None of the robberies have turned violent so far, but the I-35 Bandit is aggressive and considered extremely dangerous. Here are a few details about the serial robber:**

- He is white, middle-aged, and probably about 5' 6" tall.
- He is broad-shouldered and may be athletic—during one robbery, a security camera caught him easily vaulting a counter with one hand.
- He has no distinguishable accent but is likely a Texan judging by his knowledge of state roads and how he picks his targets.
- He chooses remote, out-of-the-way branches that typically don't have a lot of customers.
- He typically uses stolen, late-model cars and stolen license plates.
- In some of the robberies he has worn fake white beards, drawing comparisons to the lead singer for the rock band ZZ Top and also to Santa Claus.

**"Every bank robber is a serial robber unless you catch them," May said. "We need the public's help to stop this guy."**

If you have any information concerning this case, submit a tip electronically or call the FBI at this 24-hour telephone number: (210) 225-6741. There is a reward for original information leading to the identification, arrest, and conviction of the I-35 Bandit.

# Operation Bad Medicine

## Major Health Care Fraud Takedown

Last month, 153 teams led by FBI special agents and task force officers fanned out in several municipalities in Puerto Rico and arrested—without incident—about 200 of the 533 individuals named in a federal indictment involving a nearly $7 million health care fraud scheme.

Over a dozen additional defendants were arrested on the U.S. mainland and the Dominican Republic, while the 300 or so remaining subjects in Puerto Rico began to turn themselves in—at the rate of about 70 a day.

**What were they accused of?** Submitting bogus accidental injury claim forms to a large U.S. insurance company and receiving payment in return. Among those indicted was the doctor who fraudulently signed all the forms.

The January 2011 arrests were actually the second phase of Operation Bad Medicine. In December 2009, 103 individuals, including two other doctors, were indicted for the same criminal activity that resulted in the insurance company paying out more than $800,000. All 103 were convicted.

**How the case began.** Several years ago, internal auditors from the victim insurance company, which was headquartered in Atlanta, contacted our FBI office there with suspicions that certain doctors working in Puerto Rico were facilitating a scam against the company.

After our initial investigative work and the first round of indictments, we were able to identify more than 500 others involved in the same accidental injury scam against the same company. According to the January 2011 indictment, from 2004 to 2008, a doctor from Lares, Puerto Rico falsely completed and signed some of the accidental injury claim forms for policy holders and their dependants—and he pocketed approximately $450,000 for doing it.

**How the scheme worked.** In general—after word got out that this particular doctor could be bought—policy holders would go to his office claiming every sort of accidental injury imaginable. The doctor, without even examining the patient, would fill out the claim form…for a fee of between $10 to $20 per form.

The policy holders would also make fraudulent claims of accidental injuries on behalf of their kids and other family members...injuries that were never properly verified by the doctor.


**FBI investigators at the arrest command post**

The scheme became so popular that some of the policy holders became intermediaries between the doctor and other policy holders. You didn't even have to go to the doctor's office—for a $20 fee, intermediaries would carry the necessary paperwork to and from the office for you.

Once the claim form was mailed, the insurance company would send the supposed "injured" party a check within about four weeks. Which is why most of the defendants didn't just submit one claim…over time, some submitted hundreds of claims totaling thousands of dollars.

What's surprising about this case is that the defendants aren't, for the most part, hardened criminals—they are business professionals, blue collar workers, housewives, government workers, and even some law enforcement officers. But if convicted, they face up to 20 years in prison.

**Special thanks to our partners in the Social Security Administration's Office of Inspector General for their assistance during Operation Bad Medicine and to members of the Puerto Rico Police Department for their work on our arrest teams last month.**

Left: Van Thu Tran and her husband devised a plan to use a "false shuffle" to track cards and thereby guarantee successful betting. Before their ring was rounded up in 2007, some 29 casinos were hit for about $7 million.

# House of Cards

## Casino Cheating Ring Dismantled

The co-founder of a criminal enterprise known as the Tran Organization pled guilty last month to scamming casinos across the country out of millions of dollars, bringing to a close one of the largest card-cheating cases in recent FBI history.

**Van Thu Tran, 45, along with her husband, parents, extended family, and others, participated in a surprisingly simple scheme to cheat casinos at the gaming tables.**

Tran and her husband were dealers at an Indian tribal casino in San Diego in 2002 when they devised a plan to use a "false shuffle" to track cards and thereby guarantee successful betting.

"Initially, it was a pretty bare bones operation," said Special Agent Peter Casey, one of several case agents who worked the Tran investigation out of our San Diego Field Office.

Over time, the couple branched out from an Asian card game called Pai Gow to blackjack, and they enlisted many others in the scheme—including dealers at other casinos—with the promise of easy money.

For awhile, the money *was* easy, because some of the tribal casinos' security was not yet sophisticated enough to pick up on the scam. Before the ring was rounded up in 2007, some 29 casinos from Canada to Mississippi were hit for about $7 million.

**Here's how the card cheat worked:**

When signaled, the crooked dealer would make a false shuffle. Through sleight-of-hand techniques that security cameras and pit bosses failed to notice, the false shuffle created a "slug"—a group of played cards whose order would not change when the rest of the cards were shuffled. When the slug next came to the top of the deck, members of the ring recognized the card pattern and knew how to bet.

"It's a sophisticated scam, but at the same time it's simple," Casey said, "And that's why it worked so well. The organization controlled every aspect of the table."

The ring eventually began using card trackers, nearby spotters who used concealed devices to relay the order of the played cards to someone at a remote location who instantly entered the information into a computer. When the slug reappeared, the computer operator picked up the pattern and relayed it to the spotter, who then secretly signaled the bettors. One finger on a cigarette, for example, might mean bet, two fingers might mean stand pat. "It was almost like a catcher giving signs to the pitcher in baseball," Casey said. In one instance, the ring won $900,000 in blackjack during a single sitting.

**Some of the casinos realized they were being cheated, even if they weren't sure exactly how, and called the authorities.** We opened a case in 2004. But even as the Indian tribal casinos beefed up their security, the Tran Organization was hitting other casinos in the U.S. and Canada.

All the while, the ringleaders were living large. Tran and her husband had two homes in San Diego and property in Vietnam. They drove high-end vehicles and bought expensive jewelry—most of which was seized and forfeited when they were arrested.

We broke the case with the help of surveillance, wiretaps, an undercover operative posing as a crooked dealer, and strong partnerships with Internal Revenue Service investigators, the San Diego County Sheriff's Department, the California Department of Justice, and the Ontario Provincial Police.

To date, of the 47 individuals indicted in the case, 42 have entered guilty pleas to various charges.

# A Byte Out of History

## Early African-American Agents

His commanding officer was "shell shocked" from the intense fighting, his company of soldiers poorly trained and ill-equipped. Yet, as World War I drew to a close in September 1918, an African-American Army captain named James Wormley Jones fearlessly fought on, pushing forward against German forces.

**In less than 15 months, this brave officer would find himself serving the nation in another capacity—as a special agent of the Bureau of Investigation, as the FBI was known then.** We believe, in fact, that he was one of the first—if not the first—of the early African-American agents who blazed a sometimes tough trail during a difficult era.

James Jones brought plenty of experience to our young organization. He'd served for many years as a D.C. police officer prior to joining the African-American Army regiment known as the Buffalo Soldiers. And while stationed in Europe following the war, he was a senior instructor for his division's school of specialists, teaching soldiers how to handle high-powered explosives and the mechanics of bombs and grenades.

We quickly put that expertise to work. As an agent, Jones was employed exclusively in an undercover capacity, working directly under the head of the General Intelligence Division (GID), future director J. Edgar Hoover. The GID had been created a few months before in response to recent terrorist bombings, and Jones' talents and experience fit well with the division's anti-terrorist mission.

**We are aware of at least four other African-American agents who followed Jones in these early years of the Bureau:**

- **James Amos**, a former bodyguard of President Theodore Roosevelt, joined the Bureau in August 1921. He was the longest-serving of these early black agents, working some of the Bureau's biggest cases during his 32-year career.
- **Earl F. Titus**, after working as an Indianapolis police officer, joined the Bureau on January 9, 1922. His assignments included undercover work in the investigation of Marcus Garvey, a black nationalist who was convicted of mail fraud in 1923. Titus retired in June 1924 at the age of 56.

Special Agents Jesse and Robert Strider, father and son

- **Arthur Lowell Brent** became a special agent on August 1, 1923 after serving two years as a "special employee" (a sort of assistant investigator) in the Department of Justice. Brent was assigned to the Washington Field Office, where he worked on the Garvey case and other investigations. He left the Bureau in June 1924.
- **Thomas Leon Jefferson**—an experienced investigator who had worked for a detective agency in Chicago from about 1904 to 1921—entered the Bureau as an agent on September 22, 1922. Jefferson participated in many investigations, working on the Garvey case, car thefts, and prostitution/human trafficking matters. In November 1924, he was commended by Acting Director Hoover for his work on a bankruptcy investigation. Jefferson retired in January 1930.

**Over time, other African-American agents would follow these path-breakers.** Father and son agents Jesse and Robert Strider served in our L.A. office from the 1940s through the 1970s, tackling difficult fugitive investigations, military deserter matters, and other cases. They were joined in other field offices by Special Agents James Thomas Young, Harold August Carr, and Carl Vernon Mason, among others.

The careers of each of these agents, though exemplary, did reflect the struggles of the day. Unlike most investigators, some of these black agents were asked to handle lesser assignments outside their normal duties. Their struggles, though, paved the way for agents like Aubrey Lewis and James Barrow, who in 1962 became the first African-American agents accepted to the FBI Academy, ushering in a new era for minority agents in the Bureau.

Left: FBI Executive Assistant Director Shawn Henry, along with U.S. Attorney General Eric Holder, were among the officials announcing the takedown charging 111 individuals in nine cities with Medicare fraud schemes of more than $225 million.

# Health Care Fraud

## 111 Charged Nationwide

Twenty individuals, including three doctors, were charged in South Florida earlier this week for their alleged participation in a fraud scheme involving $200 million in Medicare billing for mental health services.

And that was just a precursor to today's national federal health care fraud takedown involving charges against 111 defendants in nine cities in connection with their alleged participation in schemes to bilk Medicare out of an additional $225 million. More than 700 law enforcement personnel from the FBI and Health and Human Services-Office of Inspector General (HHS-OIG), multiple Medicaid fraud control units, and other state and local law enforcement agencies took part in today's operation, which was announced at a press conference in Washington, D.C.

**HEAT.** The Florida case and the cases involved in today's takedown were the result of the Department of Justice/HHS Health Care Fraud Prevention and Enforcement Action Team, or HEAT, initiative and its Medicare Fraud Strike Force operating in a number of U.S. cities. In addition to Baton Rouge, Brooklyn, Detroit, Houston, Los Angeles, Miami, and Tampa, Attorney General Eric Holder announced at today's press conference the expansion of the strike force into two more cities—Chicago and Dallas.

Medicare Strike Force members include federal, state, and local investigators who use data analysis techniques to identify high-billing levels in health care fraud hot spots, targeting chronic fraud and emerging or migrating schemes by criminals masquerading as health care providers or suppliers.

**In the Florida case**, the indictment alleges that various defendants paid kickbacks to patient brokers and owners or operators of halfway houses and assisted living facilities for delivering patients to community mental health facilities owned by a particular corporation. The facilities would then submit claims to Medicare for services that weren't medically necessary or weren't provided at all.

**The defendants charged in today's takedown are accused of various fraud-related crimes**, including conspiracy to defraud Medicare, criminal false claims, violations of the anti-kickback statutes, money laundering, and aggravated identify theft. Some of the cases include:

- Nine charged in Houston for $8 million in fraudulent Medicare claims for physical therapy, durable medical equipment, home health care, and chiropractor services.
- Five charged in Los Angeles for a scheme to defraud Medicare of more than $28 million by submitting false claims for durable medical equipment and home health care.
- Eleven charged in Chicago for conspiracies to defraud Medicare of $6 million related to false billing for home health care, diagnostic testing, and prescription drugs.

**In addition to our involvement with HEAT and the Medicare Fraud Strike Force, the FBI remains committed to working additional health care fraud investigations with our partners** at HHS-OIG, individual state Medicare fraud offices, and investigative units from major private insurance companies. We also work jointly with the Drug Enforcement Administration, the Food and Drug Administration, and the Department of Homeland Security to address drug diversion, Internet pharmacies, prescription drug abuse, and other health care fraud threats.

**We're currently working more than 2,600 pending health care fraud investigations.** During fiscal year 2010, cooperative efforts with our law enforcement partners led to charges against approximately 930 individuals and convictions of almost 750 subjects. But perhaps even more satisfying—we dismantled dozens of criminal enterprises engaged in widespread health care fraud.

# To Catch a Fugitive

## New Tools to Find FBI's Most Wanted

For more than 60 years, the FBI has created posters to enlist the public's help in capturing fugitives or finding missing persons. Olympic bomber Eric Rudolph, CIA shooter Mir Aimal Kansi, World Trade Center bomber Ramzi Yousef—the captured fugitives were all on FBI wanted posters distributed and shared around the world.

Now, thanks to a recent redesign of the FBI.gov Most Wanted section, the public has more tools to help us close cases of suspected murderers, terrorists, bank robbers, and kidnapped and missing individuals.

For the first time, web visitors can go beyond just scanning pages of mug shots—and use search criteria like location, gender, crime type, reward, and even ZIP Codes to help narrow and focus their searches. For example, you can search for fugitives wanted for murder in California. Bear in mind, we have about 600 open cases featured on the website, and cases are removed soon after they are solved.

"Tips and leads from the public are crucial in fugitive investigations," said Special Agent Bradley Bryant, who works with local law enforcement agencies on cold cases through our Violent Crime Apprehension Program, or ViCAP. The program posts images, sketches, and profiles of individuals and their cases in hopes the public may be able to provide tips to aid investigations.

The web redesign also features a new blue profile box for each fugitive or missing person, which you can click through quickly for summaries, descriptions, aliases, photos, and more. Each profile also contains a link to the traditional poster that can be shared and printed—with printable pdfs now available for each poster.

**The profiles are now organized into three main sections:** wanted fugitives, missing persons, and seeking information. For the first time, the Wanted site also contains links to the fugitives of other federal agencies—such as the U.S. Secret Service and the Drug Enforcement Administration.

Not all FBI fugitives are included in the Most Wanted section. Many bank robbers, for example, are publicized through local Bureau press releases or through various state or local websites. See our Bank Robbery webpage for a list of those sites and additional information.

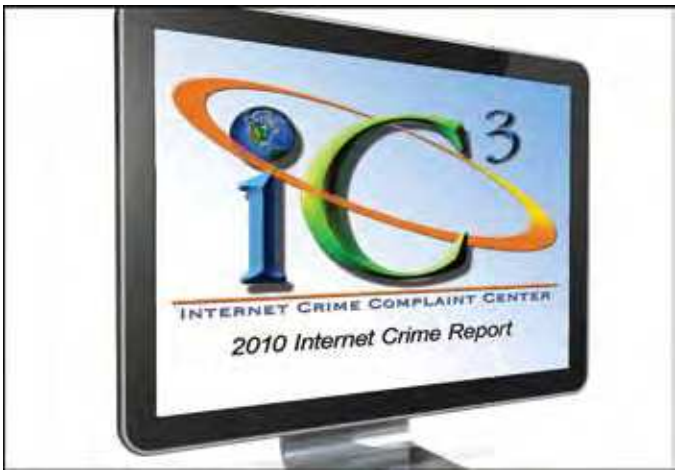

**FBI posters seeking James Earl Ray (1968), Eric Rudolph (1998), and Joe Saenz (2009)**

Early on, our fugitive posters were commonplace in federal buildings, most notably in post offices where the mug shots and rewards were as reliably present as stamp machines. In the mid-'90s, as the public's attention turned to the burgeoning Internet, FBI wanted posters followed suit. The Ten Most Wanted Fugitives list went online in 1996 with the advent of the FBI website. New categories appeared shortly thereafter, including the addition of the Most Wanted Terrorists list in 2001.

"We've come a long way from the days of distributing wanted posters," Bryant said. "We now routinely use not only the Internet, but television programs, digital billboards, and social media such as Facebook, Twitter, and YouTube to publicize wanted persons."

**To date, 56 cases have been solved as a direct result of website publicity, according to the Investigative Publicity and Public Affairs Unit, which runs the Most Wanted section.** With the evolution of FBI.gov and the Most Wanted section's new search features, we hope the public will help us even more as we move forward.

"The searchable database on our website," Special Agent Bryant says, "is in keeping with our continuing push for new and better ways to engage the public in our investigations."




# Internet Crime Trends

## The Latest Report

Non-delivery of payment or merchandise. Scams impersonating the FBI. Identity theft.

These were the top three most common complaints made to the joint FBI/National White Collar Crime Center's Internet Crime Complaint Center (IC3) last year, according to its just-released 2010 Internet Crime Report. The report also includes a state-by-state breakdown of complaints.

**In May 2010, the IC3 marked its 10th anniversary, and by November**, it had received its two millionth complaint since opening for business.

**Last year, the IC3 received more than 300,000 complaints**, averaging just over 25,000 a month. About 170,000 complaints that met specific investigative criteria—such as certain financial thresholds—were referred to the appropriate local, state, or federal law enforcement agencies. But even the complaints not referred to law enforcement, including those where no financial losses had occurred, were valuable pieces of information analyzed and used for intelligence reports and to help identify emerging fraud trends.

So even if you think an Internet scammer was targeting you and you didn't fall for it, file a complaint with the IC3. Whether or not it's referred to law enforcement, your information is vital in helping the IC3 paint a fuller picture of Internet crime.

**Additional highlights from the report:**

- Most victims filing complaints were from the U.S., male, between 40 and 59 years old, and residents of California, Florida, Texas, or New York. Most international complainants were from Canada, the United Kingdom, Australia, or India.
- In cases where perpetrator information was available, nearly 75 percent were men and more than half resided in California, Florida, New York, Texas, the District of Columbia, or Washington state. The highest numbers of perpetrators outside this country were from the United Kingdom, Nigeria, and Canada.
- After non-delivery of payment/merchandise, scams impersonating the FBI, and identity theft, rounding out the top 10 crime types were: computer crimes, miscellaneous fraud, advance fee fraud, spam, auction fraud, credit card fraud, and overpayment fraud.

**The report also contained information on some of the alerts sent out by the IC3 during 2010** in response to new scams or to an increase in established scams, including those involving:

- Telephone calls claiming victims are delinquent on payday loans;
- Online apartment and house rental and real estate scams used to swindle consumers out of thousands of dollars;
- Denial-of-service attacks on cell phones and landlines used as a ruse to access victims' bank accounts; and
- Fake e-mails seeking donations to disaster relief efforts after last year's earthquake in Haiti.

**Over the past few years, the IC3 has enhanced the way it processes, analyzes, and refers victim complaints to law enforcement.** Technology has automated the search process, so IC3 analysts as well as local, state, and federal analysts and investigators can look for similar complaints to build cases. Technology also allows law enforcement users who may be working on the same or similar cases to communicate and share information.

**Because there are so many variations of Internet scams out there, we can't possibly warn against every single one.** But we do recommend this: practice good security—make sure your computer is outfitted with the latest security software, protect your personal identification information, and be highly suspicious if someone offers you an online deal that's too good to be true.

# Help Us Catch the East Coast Rapist

## New Digital Billboard Campaign Launched

A new digital billboard campaign launched today aims to help investigators catch the "East Coast Rapist," a violent serial offender who has attacked or attempted to attack a dozen women in Maryland, Virginia, Connecticut, and Rhode Island for more than a decade.

**The billboards feature composite sketches of the rapist and a toll-free telephone number where people can call to provide information.** "These billboards give local police departments and the FBI an added edge to identify, locate, and apprehend the subject," said Ronald Hosko, special agent in charge of the Criminal Division in our Washington Field Office. "The public is the most important tool law enforcement has for solving crimes like this."

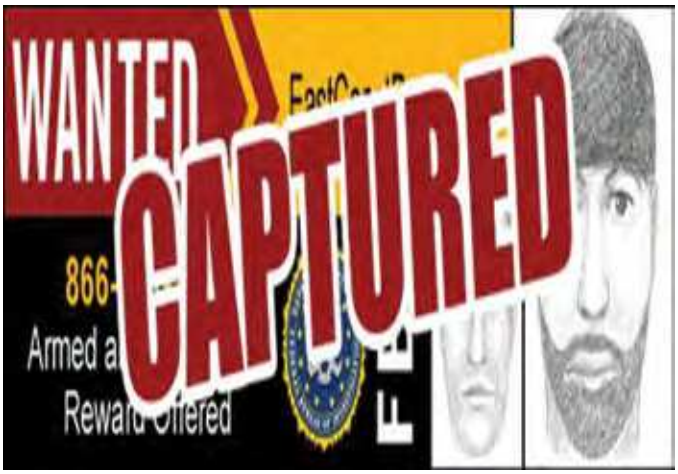
The East Coast Rapist attacked his first victim in February 1997 in a Maryland suburb of Washington D.C. He approached the 25-year-old victim on a bicycle as she walked home from work. The attacker began a conversation but then pulled a gun, forced the woman into nearby woods, and raped her.

Since then, 11 more attacks or attempted attacks have occurred. The female victims have been white, black, and Hispanic. The rapist generally approaches victims outdoors on foot and threatens them with a weapon—usually a knife or a handgun. He sometimes wears a black mask or hooded sweatshirt to conceal his face. He typically asks for money, giving victims the impression they are being robbed. But after the assault, no robbery occurs.

The attacker is described as a black male between the ages of 20 and 40 who is 5'7" to 6' tall, weighs between 150 and 200 pounds, and has a medium to muscular build. In addition to a mask and hooded sweatshirt, he has worn a variety of clothes during attacks, including green overalls, a green camouflage coat or black jacket, dark sweatpants or blue jeans, tan boots or light-colored tennis shoes, a black hair rag, and a brown or black hat.

The rapist's last known attack was in Woodbridge, Virginia on Halloween night in 2009. He raped two teenagers on their way home from trick-or-treating.

**All of the East Coast Rapist's attacks have been linked by DNA, said John Kelly, a detective with the Fairfax County Police Department in Virginia. "We have the DNA linking the offender, but we need someone to recognize and identify him."**




**The investigation involves 12 sexual assaults or attempted sexual assaults between 1997 and 2009 by the same offender. Each of the assaults is linked by DNA.**

The digital billboards will run in Maryland, Virginia, Connecticut, and Rhode Island, where the attacks and attempts have occurred, as well as in New Jersey, New York, and Delaware.

The FBI started its national digital billboard initiative in 2007 with the help of outdoor advertising companies that provide free access to more than 1,500 digital billboards in more than 40 states nationwide to publicize investigations and to provide public safety information. Since the start of the initiative, at least 39 cases have been solved as a direct result from tips from the public.

Today's campaign includes partnerships with a number of local police departments involved with the East Coast Rapist investigation. In addition to the billboards, Fairfax County Police Department has launched a dedicated website, www.EastCoastRapist.com, which provides composites and additional information about the case.

**We need your help to capture this armed and dangerous serial offender.** If you have any information regarding the East Coast Rapist, call 866-411-TIPS. Maryland's Prince George's County Police Department is offering a reward of up to $25,000 for information related to the investigation.

*Editor's note: A suspect in these cases was arrested by the East Coast Rape Task Force on March 7, 2011.*


# Operation Power Outage

## Armenian Organized Crime Group Targeted

The Southern California crime ring called Armenian Power may look like a traditional street gang—members identify themselves with tattoos and gang clothing—but the group is really an international organized crime enterprise whose illegal activities allegedly range from bank fraud and identity theft to violent extortion and kidnapping.

**Operation Power Outage—a nearly three-year investigation conducted by our Eurasian Organized Crime Task Force in Los Angeles—culminated last week with the arrests of 83 Armenian Power members on a variety of federal and state charges that include racketeering, drug trafficking, smuggling cell phones into prisons, and theft from the elderly. All told, the group allegedly bilked victims out of at least $10 million.**

In one scheme, Armenian Power—known as AP—caused more than $2 million in losses when members secretly installed "skimming" devices in cash register credit card swipe machines at Southern California 99 Cents Only stores to steal customer account information. Then they used the skimmed information to create counterfeit debit and credit cards to empty accounts.

"There is no crime too big or too small for this group," said Special Agent Louis Perez, who supervises the Eurasian Organized Crime Task Force that built the case against AP.

"This is not just a group of thugs committing crimes in their neighborhood," added Perez. "AP is sophisticated, and they have international ties. That's what sets them apart from traditional gangs."

Perez is quick to point out, though, that despite their white-collar crimes, "these are dangerous people. Just because they make money through fraud, these guys are not accountants. They use violence to get what they want," he said, explaining that one AP extortion trademark is to shoot people in the legs "to send a message."

**AP membership—thought to number about 200—consists mainly of individuals whose heritage goes back to Armenia and other Eastern Bloc countries. While the group got its start as a street gang in East Hollywood in the 1980s, AP is now less concerned with controlling neighborhood turf as it expands its criminal activities with other organized crime groups.**

For example, AP is closely allied with the Mexican Mafia, a prison gang that controls much of the narcotics distribution and other criminal activity within California's correctional facilities. AP's leadership also maintains ties to Armenia and Russia and deals directly with top organized crime figures in those countries—even to the point of using respected organized crime mediators—known as "thieves-in-law"—to settle disputes.

Steven Martinez, assistant director in charge of the FBI in Los Angeles, credits the success of the investigation and last week's takedown to the excellent partnerships between the nine local and federal agencies on the Eurasian Organized Crime Task Force. The task force consists of about 20 investigators, four of whom are FBI agents. "All the agencies involved committed their best resources," Martinez said. "The results speak for themselves."

"We think Operation Power Outage will change the face of AP," Perez added. "We took out six of their criminal cells and their leadership structure. We are confident that the repercussions of this will be felt internationally."

# Moving Money Illegally

## A $172 Million Case Example

An Oregon man recently pled guilty to operating an unlicensed money transmittal business that illegally moved more than $172 million in and out of the United States.

**As you'll read in a moment, the case is a good example of why it's important to crack down on these shady practices.**

The man behind this complex global scheme was Victor Kaganov, a former Russian military officer who emigrated to the U.S. in 1998 and eventually became a naturalized citizen. He created five "shell" corporations—businesses that only existed on paper—in Oregon and began moving money through these bogus companies for his overseas business associates.

**Money transmittal businesses in the U.S. are required by federal law to obtain a license from the state where they operate.** They are also required to register with the U.S. Treasury. Kaganov did neither.

Instead, he set up accounts under the names of his shell corporations at several Oregon banks. His overseas "clients" would generally wire transfer a substantial amount of money into one of these accounts. Then the clients—through fax or phone—would provide Kaganov with instructions on where to further transmit the funds.

From 2002 to 2009, Kaganov facilitated more than 4,200 wire transactions. A significant portion of the funds transferred into his accounts came from Russia, but the money was transferred out to 50 other countries, mostly in Asia and Europe.

**Cooperation was key in this case—we were greatly assisted by the U.S. Treasury, our overseas legal attachés, and our global law enforcement partners.**

The Kaganov investigation was a spinoff of a broader FBI case investigating the use of Oregon shell corporations by overseas businesses and individuals to move illicit funds.

Another spinoff of the broader FBI investigation is a brand new hybrid investigative squad in our Portland office focused on any and all threats from Eurasian criminals—one of the FBI's top organized crime priorities. We call it a "hybrid" squad because it includes agents and analysts from Bureau programs across the board—organized crime, counterterrorism, intelligence, cyber, and counterintelligence.

**Why are licensing and registration laws so important?** Several years ago, the U.S. government issued a money-laundering assessment that identified money services businesses—especially wire remitters—as a chief conduit for the illicit transmission of money, including funds used to finance all sorts of criminal activity and terrorism. Requirements to register these businesses enable state and federal regulatory agencies to keep a closer eye on what they're doing.

And whether or not the funds moved through these businesses came from or funded illegal activity, there is other fallout from these businesses. For example, the bank accounts used to facilitate the transfer of money see an awful lot of activity—in Kaganov's case, there were daily and sometimes even hourly transactions—and that has the potential to destabilize banks. Also, creators of shell corporations often don't file any tax returns, so they remain unknown to taxing authorities. Or, they keep two sets of financial books—one that they show to taxing authorities and the real one that never sees the light of day.

By thwarting laws and regulations that govern the U.S. financial system, criminals can undermine its integrity. The FBI and its partners are working hard to make sure that doesn't happen.

Left: FBI Executive Assistant Director Shawn Henry, with Attorney General Eric Holder, holds up a Most Wanted poster of Barrio Azteca gang leader Eduardo Ravelo during a press conference in Washington, D.C. announcing charges against the gang in the U.S. Consulate murders last March.

# Violent Border Gang Indicted

## Members Charged in Consulate Murders

Thirty-five leaders, members, and associates of one of the most brutal gangs operating along the U.S.-Mexico border have been charged in a federal indictment in Texas with various counts of racketeering, murder, drug offenses, money laundering, and obstruction of justice.

Of the 35 subjects, 10 Mexican nationals were specifically charged with the March 2010 murders in Juarez, Mexico of a U.S. Consulate employee and her husband, along with the husband of another consulate employee.

The indictment was announced today at a press conference in Washington, D.C., by U.S. Attorney General Eric Holder, FBI Executive Assistant Director Shawn Henry, and other representatives. All commented on the cooperation American officials received from their Mexican counterparts. Said Henry, "We may stand on opposite sides of the border, but we stand together on the same side of the law."

Seven of the 10 charged with the U.S. Consulate murders —and two other indicted defendants—are in custody in Mexico. Three remain at large, including Eduardo Ravelo, currently one of the FBI's Top Ten Most Wanted Fugitives. We're offering a reward of up to $100,000 for information leading directly to his arrest.

The Barrio Azteca began in the late 1980s as a prison gang but has since expanded into a transnational criminal organization with approximately 3,500 members, including 600 active members located in West Texas and Juarez, Mexico. Barrio Azteca gang members can also be found throughout state and federal prisons in the U.S. and Mexico.

This particular organization is known to engage in criminal activities both inside and outside of prison walls. Those activities include murder, assault, threats of violence, extortion, money laundering, witness intimidation, illegal firearms possession, alien smuggling, and drug trafficking—on both sides of the U.S.-Mexico border.

**According to today's indictment, the Barrio Azteca formed an alliance with the Vicente Carrillo-Fuentes (VCF) drug trafficking organization in Mexico**, conducting enforcement operations against VCF rivals and receiving "discounts" on illegal drugs from the VCF.

And in addition to the consulate murders, the defendants are allegedly responsible for a number of other murders in the U.S. and Mexico. The indictment states they also imported heroin, cocaine, and marijuana into the U.S. and charged a "cuota," or tax, on businesses and other criminals operating on their turf. The funds raised by these taxes were allegedly funneled into prison commissary accounts of gang leaders and also helped pay for defense lawyers.

**Today's indictment is a direct result of the cooperation among the local, state, and federal law enforcement agencies and prosecutors involved.** Members of our multi-agency Safe Streets Task Forces out of our El Paso and Albuquerque offices worked seamlessly with one another throughout the investigation, sharing intelligence, conducting surveillance, making undercover drug buys, and executing search warrants.

The use of Safe Streets Task Forces is part of our strategy for going after these violent criminals—we currently have 168 Violent Gang Task Forces and 41 Violent Crime Task Forces nationwide. Also valuable is our ability to use federal statutes, because they often result in longer sentences and allow us to seize and forfeit assets from convicted gang members. And targeting the leadership of these criminal groups often disrupts their ability to ply their illegal trade.

Hopefully, with today's indictment and arrests, the streets on both sides of the border are a little safer.

# Domestic Security

## Combating Crime, Protecting Commerce

Five American-based corporations received threatening phone calls for more than a year. The threats were reported to various authorities, but the culprit wasn't identified.

Then, a sixth company received a threatening phone call. Fortunately, that company was a member of the Domestic Security Alliance Council (DSAC), a security and intelligence-sharing initiative between the FBI, the Department of Homeland Security (DHS), and the private sector. The company's chief security officer contacted DSAC's program office in Washington, D.C., to relay the incident. In less than 10 days, a DSAC analyst—working with FBI field offices—connected the dots that led to the identification of a suspect.

**DSAC works to prevent, detect, and investigate criminal acts**—particularly those affecting interstate commerce—while helping the private sector protect its employees, assets, and proprietary information. It's similar to the Bureau's InfraGard program, which brings together representatives from the private and public sectors to help protect our nation's critical infrastructure and key resources from terrorists, criminals, and others.

Through open lines of communication, DSAC ensures that key senior private sector executives and senior government officials share real-time, actionable intelligence.

**DSAC was modeled after the Overseas Security Advisory Council**—started pre-9/11 by the State Department to exchange information with U.S. private sector firms, many of whom operate overseas, concerning international security issues. After 9/11, it became clear that a similar initiative was needed to encourage the exchange of information on domestic security issues. And the FBI took the lead in setting it up, with DHS acting as a key partner today.

According to program director Daniel DeSimone, "DSAC bridges the information-sharing divide between the public and private sector" on the many security threats facing today's businesses. "Threats," explained Arnold Bell, DSAC deputy program director, "like a foreign national trying to covertly acquire sensitive information or technology, a trusted employee willing to sell a company's secrets, or IT experts or other personnel using ineffective practices that result in security breaches."


**Currently, DSAC consists of nearly 200 diverse U.S. companies and organizations**—and that number continues to grow. Although vigilant about terrorist and counterintelligence threats, the day-to-day security concerns of these entities primarily involve criminal threats—like computer intrusions, workplace violence, insider threats, fraud, trade secret theft, and product tampering. And DSAC personnel work closely with each of the Bureau's operational divisions.

**Services offered to DSAC members include:**

- **An interactive website** (www.dsac.gov) that posts weekly intelligence briefs and other unclassified information from the FBI and other U.S. intelligence agencies, analytical products from member companies, news feeds, a resource library, and an online meeting capability;
- **The Domestic Security Executive Academy** that brings together corporate chief security officers and senior U.S. government officials to build strategic partnerships and discuss the latest criminal and domestic security issues affecting U.S. commerce; and
- **Intelligence Analyst Symposiums** that provide joint training for corporate security analysts, U.S. government intelligence analysts, and federal, state, and local law enforcement partners on intelligence tradecraft, methodologies, and best practices.

Most recently, the DSAC program has been brought under the umbrella of the Director's Office, teamed with our Office of Law Enforcement Coordination (OLEC), which is responsible for building bridges, strengthening relationships, and sharing information with our public sector law enforcement partners. Said OLEC Assistant Director Ronald Ruecker, "Performing similar activities with our private sector partners is a logical extension of OLEC's mission."

# Serial Scammer

## Targeted L.A. Latino Community

Last month, a California con man was sentenced to 22 years in prison for running a Ponzi scheme that raked in at least $30 million from more than 500 victims and for launching a mortgage fraud operation that targeted distressed homeowners.

The man behind these scams—a Mexican national living in the U.S.—did most of that damage by purposely targeting mostly working-class, Spanish-speaking victims in Los Angeles.

And at Juan Rangel's sentencing hearing, more than a dozen victims addressed the court, including one investor who had been convinced to invest money she received after her son was killed while serving as a U.S. soldier in Iraq.

**The Ponzi scheme.** Rangel's company—Financial Plus Investments—was never licensed by the U.S. Securities and Exchange Commission, but that didn't stop him from offering investments with guaranteed returns as high as 60 percent annually.

Rangel solicited investors from Los Angeles through Spanish-language newspapers and magazines, radio advertisements, television infomercials, and investment seminars.

He told potential investors that his company earned profits from real estate-related investments and that if they invested with him, their money would be used to buy, renovate, and sell properties…and make high-interest rate loans to homeowners who were facing foreclosure. But what they didn't know was that Rangel was using their money to pay off prior investors and fund a $2.5 million mansion and luxury sports car.

But, as all Ponzi schemes do eventually, Rangel's scam—which started around November 2007—began collapsing in on itself when he didn't have enough new investors to pay off the old ones. Checks stopped going out, and Financial Plus closed its doors in July 2008.

**The mortgage fraud scheme.** For approximately two years before, Rangel and his Financial Plus vice-president—who was also charged in this scheme—identified homeowners who were in default on their mortgages but who still had substantial equity remaining in their properties. Spanish-speaking Financial Plus employees were then directed to make unsolicited visits to identified homeowners with Latino surnames.

Rangel and his vice president would then meet with the homeowners who were interested in Financial Plus' offer to help them avoid foreclosure. Some homeowners were told that Financial Plus would refinance their properties with another lender using a "co-signer" who had good credit. Others were told that Financial Plus would arrange for temporary sales of the properties, that the titles would be transferred but they could still live in the home, and that the titles would be returned to them after a year or less.

Of course, in both instances, the homeowners ended up with nothing….while Financial Plus ended up with the proceeds from fraudulently obtained loans and titles to homeowners' properties.

The case was investigated by the FBI and our partners at the U.S. Postal Inspection Service and the Internal Revenue Service's Criminal Investigation Division.

**When it came time to arrest Rangel after his October 2010 indictment on the Ponzi and mortgage fraud schemes, law enforcement authorities didn't have to look that far**—he was already in federal custody after his 2009 conviction for bribing a bank manager to falsify bank documents in direct support of his mortgage fraud scheme.

**Moral of the story?** When turning over your hard-earned money or property, make sure you do your due diligence on the people who are taking it.

# Cryptanalysts

## Part 1: Breaking Codes to Stop Crime

The letter from a gang member in prison to a friend on the outside seemed normal enough. "Saludos loved one," it began, and went on to describe the perils of drug use and the inmate's upcoming visit from his children.

**But closer inspection by examiners in our Cryptanalysis and Racketeering Records Unit (CRRU) revealed that this seemingly ordinary letter was encoded with a much more sinister message: every fifth word contained the letter's true intent, which was to green-light the murder of a fellow gang member.**

Breaking such codes is CRRU's unique specialty. Despite the FBI's extensive use of state-of-the-art computer technology to gather intelligence, examine evidence, and help solve crimes, the need to manually break "pen and paper" codes remains a valuable—and necessary—weapon in the Bureau's investigative arsenal.

That's because criminals who use cryptography—codes, ciphers, and concealed messages—are more numerous than one might expect. Terrorists, gang members, inmates, drug dealers, violent lone offenders, and organized crime groups involved in gambling and prostitution use letters, numbers, symbols, and even invisible ink to encode messages in an attempt to hide illegal activity.

Bookies, pimps, and drug traffickers, for example, all keep records of their dealings, explained Dan Olson, chief of CRRU, which is part of the FBI Laboratory. "If there is money and credit involved in a transaction," Olson said, "there has to be an accounting of that at every step of the way, even if it's on a match pack, hotel stationary, or the back of a cocktail napkin."

The unit's forensic examiners are often tasked with decoding encrypted evidence after subjects have been arrested. But CRRU also plays an important role in thwarting crime by intercepting coded messages—like the prison letter above—particularly among inmates and gang members. "We solve crimes," Olson said, "but we actually prevent more crimes than we solve."

The art of breaking codes is an "old-fashioned battle of the minds" between code makers and code breakers, Olson added, explaining that CRRU is the only law enforcement unit anywhere that deals exclusively with manual—as opposed to digital—code breaking.

1 2 3

SALUDOS LOVED ONE

4 5 1 2 3 4 5 ...

SO TODAY I HEARD FROM UNCLE MIKE OVER THE PHONE. HE TOLD ME THAT YOU AND ME GO THE SAME BIRTHDAY. HE SAYS YOUR TIME THERE TESTED YOUR STRENGTH SO STAY POSITIVE AT SUCH TIMES. I'M FOR ALL THAT CLEAN LIVING! METHAMPHETAMINES WAS MY DOWN FALL. THE PROGRAM I'M STARTING THE NINTH IS ONE I HEARD OF A COUPLE WEEKS BEFORE SEPTEMBER THROUGH MY COUNSELOR BARRIOS. BUT MY MEDICAL INSURANCE COVERAGE DENIES THEY COVER IT. I'M USING MY TIME TO CHECK AND IF THE INSURANCE AGENT DENIES STILL MY COVERAGE I'M GETTING TOGETHER PAPERWORK SAYING I TESTED FOR THIS TREATMENT REQUIRED ON THE CHILD CUSTODY. THE NINTH WILL MEAN I HAVE TESTED MY DETERMINATION TO CHANGE. ON THE NEXT FREE WEEKEND THE KIDS ARE COMING, BUT FIRST I GOTTA SHOW CAROLINA I'M STAYING OUT OF TROUBLE WAITING TO GET MYSELF ADMITTED ON THE PROGRAM. THE SUPPORTING PAPERWORK THAT THE FAMILY COURTS GOT WILL ALSO PROVE THERE'S NO REASON NEITHER FOR A WITNESS ON MY CHILDREN'S VISITS. OF COURSE MY BRO HAS HIS MIND MADE UP OF RECENT THAT ALL THIS DRUG USAGE DON'T CONCERN OUR VISITS. I THINK THAT MY KIDS FEEL I NEED THEIR LOVE IF I'M GONNA BE COOL. GUILTY FEELINGS RISE ON ACCOUNT OF THE MISTAKES I COULD WRITE UP. FOR DAYS I'M HERE. HE GOT A GOOD HEART. SHOULD YOU BE HAVING PROBLEMS BE ASSURED THAT WHEN YOU HIT THE STREETS WE'LL BE CONSIDERING YOU!

Encrypted letter from imprisoned gang member

**"We would love to find our counterparts somewhere in the world," he said, "but so far we haven't been able to. No one seems to have the niche that we have."**

Becoming a cryptanalyst requires a basic four-month training course and plenty of continuing education to learn the age-old patterns and techniques of code makers. Olson insists that almost anyone can learn basic code-breaking skills, but certain personality types seem best suited to the job, including those who like solving puzzles and who are determined and tenacious.

The unit's examiners include linguists, mathematicians, and former law enforcement officers like Debra O'Donnell, who worked drug and gang cases in New Jersey before joining the Bureau. "This is very rewarding work," O'Donnell said, "but you have to have the right temperament for it, because you can't break every code."

Still, since World War II, when Bureau cryptanalysts were responsible for cracking Nazi spy codes, CRRU has been getting results—not only for FBI cases but also for local, state, and federal investigators who request our training and assistance.

"We've evolved with the crime trends over the years," Olson said, "but at the same time we've kept our previous missions. As long as there are criminals," he added, "there will be a need for cryptanalysts."

Left: FBI Director's Community Leadership Awards

# Improving Communities

## Leaders Honored in Washington

They come from different parts of the country. They work in many different fields. And they serve a variety of constituencies.

But the 50-plus individuals who gathered at FBI Headquarters in Washington, D.C., today for a special ceremony have one thing in common: they are all recipients of the 2010 Director's Community Leadership Award (DCLA) for their selfless actions within their communities. And, according to Director Robert Mueller, the recipients share "a willingness to lead and a commitment to improve the lives of their neighbors.... They embody the true meaning of citizenship."

**This year's recipients show how ordinary citizens can make such a big difference in the lives of others**, from the New Mexico Anti-Defamation League regional director who combats prejudice and discrimination…to the mosque board member in Cincinnati who educates law enforcement and community leaders about the Muslim faith…from the New Jersey child advocate dedicated to protecting kids from online sexual predators…to the Seattle television anchor whose news program highlights and helps apprehend dangerous fugitives.

And those who benefit from their involvement also represent a broad spectrum of the community, including the young, the elderly, the disabled, women and girls, refugees and legal immigrants, crime victims, minority groups, law enforcement, and the general public.

**We present each of these awards publicly**—first at the local FBI field office and then at a national ceremony in Washington—with the hopes that others will hear the stories of the recipients and be inspired to create change in their own communities, working to keep their neighborhoods safer.

**Here are a few more examples of the individuals and organizations selected to receive the DCLA:**

- An Arkansas woman who became a tireless advocate for the elderly after members of her family experienced nursing home abuse;
- An organization in Buffalo that provided resources and assistance to victims who came to light during an FBI human trafficking investigation;
- A former NASA astronaut and successful businessman in Houston who established a foundation that invests in community-based initiatives that empower individuals, particularly minorities and the economically disadvantaged;
- A former deputy fire chief from Louisville who promotes emergency preparedness among first responders and members of the public;
- A St. Louis doctor who risked his career to help uncover massive Medicare and Medicaid fraud being perpetrated by the health care company he worked for; and
- A county school employee in Tampa who created a program for at-risk young males that is now used by the state attorney's office as a diversion program for first-time offenders.

Every year, FBI field offices select individuals or organizations—one per office—to receive the DCLA. The criteria for the award? Achievements in combating terrorism, cyber crime, and illegal drugs, gangs, and other crimes; or violence prevention/education efforts that have had a tremendous positive impact on their communities. This year's crop of award recipients joins the ranks of a dedicated group of people and organizations that, since 1990, have collectively enhanced the lives of thousands of individuals and families and helped protect communities around the United States.

Congratulations to the winners!

# Cryptanalysts

## Part 2: Help Solve an Open Murder Case

On June 30, 1999, sheriff's officers in St. Louis, Missouri discovered the body of 41-year-old Ricky McCormick. He had been murdered and dumped in a field. The only clues regarding the homicide were two encrypted notes found in the victim's pants pockets.

**Despite extensive work by our Cryptanalysis and Racketeering Records Unit (CRRU), as well as help from the American Cryptogram Association, the meanings of those two coded notes remain a mystery to this day, and Ricky McCormick's murderer has yet to face justice.**

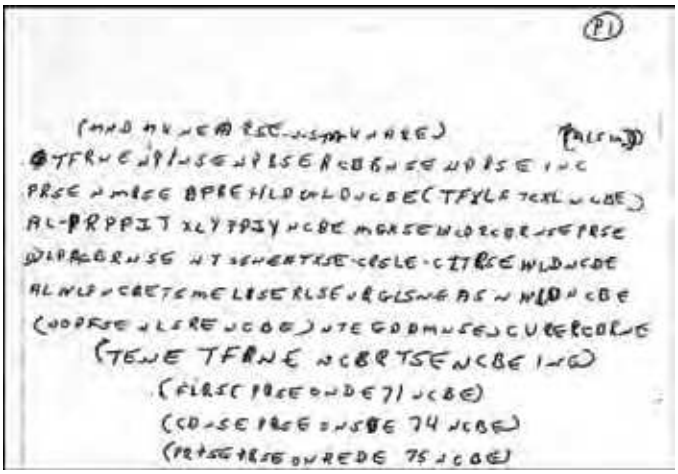
"We are really good at what we do," said CRRU chief Dan Olson, "but we could use some help with this one."

In fact, Ricky McCormick's encrypted notes are one of CRRU's top unsolved cases. "Breaking the code," said Olson, "could reveal the victim's whereabouts before his death and could lead to the solution of a homicide. Not every cipher we get arrives at our door under those circumstances."

**The more than 30 lines of coded material use a maddening variety of letters, numbers, dashes, and parentheses.** McCormick was a high school dropout, but he was able to read and write and was said to be "street smart." According to members of his family, McCormick had used such encrypted notes since he was a boy, but apparently no one in his family knows how to decipher the codes, and it's unknown whether anyone besides McCormick could translate his secret language. Investigators believe the notes in McCormick's pockets were written up to three days before his death.

Over the years, a number of CRRU's examiners—who are experts at breaking codes—have puzzled over the McCormick notes and applied a variety of analytical techniques to tease out an answer. "Standard routes of cryptanalysis seem to have hit brick walls," Olson noted. Our cryptanalysts have several plausible theories about the notes, but so far, there has been no solution.

To move the case forward, examiners need another sample of McCormick's coded system—or a similar one—that might offer context to the mystery notes or allow valuable comparisons to be made. Or, short of new evidence, Olson said, "Maybe someone with a fresh set of eyes might come up with a brilliant new idea."



The meanings of the coded notes remain a mystery to this day.

**That's where the public comes in.** The FBI has always relied on tips and other assistance from the public to solve crimes, and although breaking a code may represent a special circumstance, your help could aid the investigation. Take a look at McCormick's two notes. If you have an idea how to break the code, have seen similar codes, or have any information about the Ricky McCormick case, send them to us online at *http://forms.fbi.gov/code* or write to CRRU at the following address:

FBI Laboratory
Cryptanalysis and Racketeering Records Unit
2501 Investigation Parkway
Quantico, VA 22135
Attn: Ricky McCormick Case

There is no reward being offered, just a challenge—and the satisfaction of knowing that your brain power might help bring a killer to justice.

"Even if we found out that he was writing a grocery list or a love letter," Olson said, "we would still want to see how the code is solved. This is a cipher system we know nothing about."

# FBI Records

## New 'Vault' Comes Online

Last April, we launched a complete overhaul of our FBI Records/Freedom of Information and Privacy Act website, including a new electronic form for submitting requests.

Now, we are announcing a revamping of our electronic reading room—renamed "The Vault"—which contains more than two thousand documents that have been scanned from paper into digital copies so you can read them in the comfort of your own home or office.

Included here are more than 25 new files that have been released to the public but never added to this website; dozens of records previously posted on our site but removed as requests diminished over time; and files carried over from our previous electronic reading room.

The Vault includes several new tools and resources for your convenience:

- **Searching for topics:** You can browse or search for specific topics or persons (like Al Capone or Marilyn Monroe) by viewing our alphabetical listing, by using the search tool in the upper right of this site, or by checking the many different category lists that can be found in the menu on the right side of the page.
- **Searching for key words:** Thanks to new technology we have developed, you can now search for key words or phrases **within** some individual files. You can search across all of our electronic files by using the search tool in the upper right of this site, or you can search for key words within a specific document by typing in terms in the search box in the upper right-hand corner of the file after it has been opened and loaded. Note: since many of the files include hand-written notes or are not always in optimal condition due to age, this search feature does not always work perfectly.
- **Viewing the files:** We are now using an open source web document viewer, so you no longer need your own file software to view our records. When you click on a file, it loads in a reader that enables you to view one or two pages at a time, search for key words, shrink or enlarge the size of the text, use different scroll features, and more. In many cases, the quality and clarity of the individual files have been improved as well.
- **Requesting a status update:** Use our new Check the Status of Your Freedom of Information and Privacy Act (FOI/PA) Request tool to determine where your request stands in our process. Status information is updated weekly. Note: You need your FOI/PA request number to use this feature.

"The new website significantly increases the number of available FBI files, enhances the speed at which the files can be accessed, and contains a robust search capability," says David Hardy, chief of the Record/Information Dissemination Section in our Records Management Division. "It reflects a strong commitment to build public trust and confidence through greater public access to FBI records."

We'll be adding more files to the Vault each month, so check back often.

And, as always, if you have questions about requesting FBI records or related issues, call our Freedom of Information Act Requestor Service Center at (540) 868-1535 to hear helpful recorded information, or contact our Record/Information Dissemination Section.

# Private Tender

## Anti-Government Group Mints Its Own Coins

Money doesn't grow on trees. It also can't be printed or minted by private citizens—as four co-conspirators in North Carolina and Indiana recently learned the hard way.

Last month, the founder and "monetary architect" of an illegal currency known as the Liberty Dollar was convicted in North Carolina on federal charges of making illegal coins and selling them—at a profit—to compete with legal U.S. currency. Bernard von NotHaus, of Evansville, Indiana, was found guilty of making coins resembling U.S. coins; issuing, passing, selling, and possessing Liberty Dollar coins; issuing and passing Liberty Dollar coins intended for use as current money; and conspiring against the United States. Three others indicted in the case are awaiting their own trials.

"People understand that there is only one legal currency in the United States," said Owen Harris, then-special agent in charge of our office in Charlotte. "When groups try to replace it with coins and bills that don't hold the same value, it affects the economy. And consumers were using their hard-earned money to buy goods and services, then getting fake goods in return."

**It all began in 2004**, when our Charlotte Division learned that a customer at a North Carolina financial institution had tried to use silver coins that were not legal U.S. currency. Our investigation revealed that the coins came from the National Organization for the Repeal of the Federal Reserve and Internal Revenue Codes (or NORFED), headquartered in Evansville, whose mission was to return the country's monetary system to gold and silver. The president of the organization was Bernard von NotHaus, who marketed his currency as inflation-proof, claimed it was backed by silver and gold, and said it could be used to compete with—and limit reliance on—U.S. currency.

Our investigation, which included an undercover scenario, revealed that NORFED contracted for the minting of about $7 million worth of Liberty Dollars in Idaho. The organization also took orders and payments from customers for Liberty Dollars and organized "Liberty Dollar University" sessions to help educate people interested in selling, buying, or using the currency. There was even a Liberty Dollar website.


**During the investigation, the U.S. Mint warned that Liberty Dollar coins were not legal tender.**

**NORFED used several groups of people to get its illegal coins into circulation:**

- Regional currency officers marketed Liberty Dollars in their geographic areas.
- Liberty Dollar associates paid a $250 membership fee and received 100 Liberty Dollars, plus instructions on how to market the currency.
- Recruited merchants and business owners accepted Liberty Dollars in exchange for goods or services and handed out the coins as change.

**During the course of the investigation, the U.S. Mint issued a press release warning that the Liberty Dollar was not legal tender** and that the Department of Justice had determined that the use of these coins as circulating money was a federal crime. This press release was sent to known NORFED regional currency officers. Despite the warning, though, NORFED and its officers, members, and associates continued to break the law and circulate the illegal tender.

**As with many of our other cases, we didn't work this investigation alone.** Providing tremendous assistance was the Buncombe County Sheriff's Office, U.S. Secret Service, U.S. Treasury's Office of Inspector General for Tax Administration, North Carolina Joint Terrorism Task Force, U.S. Postal Inspection Service, and U.S. Mint.

# Intelligence in Action

## The Director's Briefer

It's 1 a.m. on a Tuesday morning, and Colleen Stewart (not her real name) is settling in on the 11th floor of FBI Headquarters. Most of the country's asleep. But for Stewart, it's time to log into a half-dozen top secret databases and make sense of the moment's most pressing threats against the U.S., its citizens, and its allies.

Over the next eight hours, Stewart will review and research dozens of threat analyses. Then she'll distill them into a narrative to deliver in morning briefings to the Director, the Attorney General, and the FBI's top counterterrorism officials. The intelligence is developed across the breadth of U.S. intelligence agencies, including from within the Bureau. But it falls on one intelligence analyst detailed to the FBI's Directorate of Intelligence to boil it down to a coherent 20-minute morning briefing. The pace of the job is intense, weighted by the analyst's singular responsibility and the gravity of time-sensitive intelligence.

"Not getting things done is not an option," says Stewart, the Director's intelligence briefer for the past year. "The Director is expecting you to have gone through the reports and pulled out the important information."

The reports are developed by FBI intelligence analysts and partner agencies, like the CIA, NSA, and the National Counterterrorism Center (NCTC), and disseminated across the intelligence community. The reports are complied into a book that Stewart will be expected to know cover-to-cover by morning.

Around 2 a.m., NCTC issues its latest report. The briefer's challenge is to glean the most important items to highlight, while at the same time having a sense of the Director's depth of knowledge to avoid wasting time.

**The intelligence briefer position resulted in part from post-9/11 reforms that called for better communications among intelligence agencies.** In 2003, as agencies increased sharing, the Bureau first enlisted an FBI intelligence analyst with deep counterterrorism experience to deliver the Director's briefing. Today, briefers like Stewart and others who keep the Director abreast of events throughout the day can easily access partner agency databases with a keyboard and mouse.

"Who is this guy?" Stewart says to herself, her eyes trained on her monitor. "I recognize this face." It's 3 a.m., and she's looking at a rap sheet of sorts on a suspected terrorist she's seen before, but the name is new. She consults a binder containing charts she's amassed to help visually connect the dots. Then she sees it. "That's who … ok … aha."

Stewart, 35, has always been interested in law enforcement. She studied criminology and interned with the FBI's Behavioral Analysis Unit before joining the Bureau in 2008. She was a public corruption analyst before responding to a call last year for candidates interested in the year-long briefer assignment.

**"I thought, 'Who wouldn't want to do that job?'"** Stewart says.

By 4:20 a.m., the night's intelligence reports are organized in binders for the Director, the Attorney General, their staffs, and leadership across the Counterterrorism Division. The Director's book is hand-delivered around 5:30 a.m., giving him a couple hours to review it before he's briefed.

At 6 a.m., Stewart stows the food she never got around to eating. She changes from sweats into a dark suit and runs through a mental checklist of the last five hours.

At 6:50 a.m. Stewart pre-briefs her bosses to shore up her presentation before briefing—in succession—the Counterterrorism Division, Director Mueller, and Attorney General Eric Holder. Briefings aren't passive, so Stewart makes sure she has answers to potential questions and has invited subject-matter experts who sit in to support their analyses. The result: critical information gets delivered directly to decision-makers who need it to shape how the FBI responds to the most pressing threats.

**"What the briefers do is critical," says Mark Giuliano, head of the FBI's Counterterrorism Division.** "They find the intel that rises above the other noise, put context to it, and share it with the people who need it. Analysts and briefers really know how it all fits together, and that's where the value is added."

# A Byte Out of History

## Fatal Firefight in Miami

On the morning of April 11, 1986—25 years ago today—one of the deadliest and most violent shoot-outs in FBI history unfolded just outside of the city of Miami.

**FBI agents were leading a massive manhunt for two violent bank robbers—later identified as Michael Lee Platt and William Russell Matix—who were known for using high-caliber firearms and stolen cars.** They had murdered several people since the previous October, and Miami police and the FBI were closing in on them.

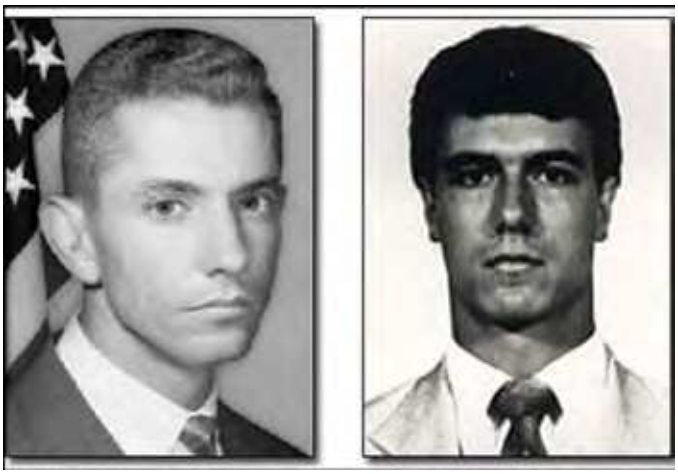
Miami Special Agents Benjamin Grogan and Jerry Dove—two of the eight agents ultimately directly involved in the firefight who were riding together in one of the five pursuing Bureau cars—noticed a stolen, black Monte Carlo connected to the two robbers and began following it.

Also in close pursuit and riding alone, Special Agent Richard Manauzzi tried to steer the Monte Carlo into a tree at the side of 12201 SW 82nd Avenue when he noticed one of the criminals aiming a weapon toward pursuing FBI agents. Three Bureau cars collided with the suspects and forced them off the road, but the felons opened fire.

**The events unfolded quickly and horrifically.** Special Agent Manauzzi was seriously wounded and immediately sought cover. Special Agent Gordon McNeill—also riding alone—was wounded, but returned fire, striking Matix. Special Agents Gilbert Orrantia and Ronald Risner were pinned in their vehicle on the other side of the street; Orrantia was wounded. Special Agents Edmundo Mireles and John Hanlon had also stopped their car on the opposite side of the street and came under high-powered rifle fire as they tried to approach the felons. Both were seriously wounded. Special Agents Dove and Grogan—despite wounding both criminals in the hail of bullets—were trapped in their car and killed when Platt fired at close range. Platt also shot and incapacitated Agent Hanlon.

Severely wounded and struggling to remain conscious, Special Agent Mireles stood up and began firing at the criminals as they entered and tried to escape in Dove and Grogan's car. He killed both men even as they returned fire.

**In the end, the FBI's casualties were higher than any shoot-out in its history:** two dead, three seriously wounded, and two others injured. Only Agent Risner was unhurt.



Miami FBI Special Agents Benjamin Grogan, left, and Jerry Dove

In the aftermath of the gun battle, the FBI and other law enforcement agencies closely studied the incident. Although wounded, both Platt and Matix were able to continue firing their weapons at the surrounding agents. Our guns had not stopped them. Furthermore, the killers' weapons were more powerful and their rounds could penetrate even the armored vests that some of the agents were wearing.

In response to this tragedy, the FBI made significant changes in the firepower carried by agents, the body armor they wore, and the incident response training they received.

**Today, we honor not just Agents Dove and Grogan—and their colleagues injured that day—but all of the men and women of the FBI who have given their lives in the line of duty and put themselves in harm's way to protect their communities.** As Director Mueller said in a ceremony in Miami attended by former FBI Director William Webster, survivors of the shooting, and many others:

"It has been said that all great things are simple, and most can be expressed in a single word: fidelity, bravery, and integrity. Honor, duty, and sacrifice. But it is no simple matter to act on such words when every second counts and life hangs in the balance. The individuals we honor today embodied the true meaning of these words and what it means to be a special agent."

Left: Botnets are networks of virus-infected computers controlled remotely by an attacker. The Coreflood virus is a key-logging program that allows cyber thieves to steal personal and financial information by recording unsuspecting users' every keystroke.

# Botnet Operation Disabled

## FBI Seizes Servers to Stop Cyber Fraud

In an unprecedented move in the fight against cyber crime, the FBI has disrupted an international cyber fraud operation by seizing the servers that had infected as many as two million computers with malicious software.

Botnets are networks of virus-infected computers controlled remotely by an attacker. They can be used to steal funds, hijack identities, and commit other crimes. The botnet in this case involves the potent Coreflood virus, a key-logging program that allows cyber thieves to steal personal and financial information by recording unsuspecting users' every keystroke.

Once a computer or network of computers is infected by Coreflood—infection may occur when users open a malicious e-mail attachment—thieves control the malware through remote servers. The Department of Justice yesterday received search warrants to effectively disable the Coreflood botnet by seizing the five U.S. servers used by the hackers.

**"Botnets and the cyber criminals who deploy them jeopardize the economic security of the United States and the dependability of the nation's information infrastructure," said Shawn Henry, executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch.** "These actions to mitigate the threat posed by the Coreflood botnet are the first of their kind in the United States," Henry noted, "and reflect our commitment to being creative and proactive in making the Internet more secure."

Now that we have interrupted the operation of the botnet servers, our cyber specialists can prevent Coreflood from sending stolen financial information to the cyber thieves. But victims' computers still remain infected. That's why we have been working closely with our private-sector partners.

**Anti-virus companies are developing updated signatures to detect and remove Coreflood. To disinfect Microsoft Windows-based systems—and to keep them virus free—users are encouraged to run anti-virus software and to keep their Microsoft Windows Updates current.**

Victimized computers that have not been disinfected using anti-virus software updates will continue to attempt to contact the Coreflood botnet servers. When this happens, we will respond by issuing a temporary stop command to the virus and then alert that user's Internet service provider (ISP), who will inform the customer that their computer is still infected. At no time will we be collecting any personal data from victim computers.

"For most infected users who are conscientious about keeping their anti-virus programs up to date, the process of disinfection will be as invisible as the Coreflood infection was itself," said one of our cyber agents. Still, there is a process in place with ISPs to make sure notification occurs if necessary.

**We began our Coreflood investigation in April 2009 when a Connecticut-based company realized that hundreds of computers on its networks had been infected.** Before we shut down the Coreflood operation, cyber thieves made numerous fraudulent wire transfers, costing companies hundreds of thousands of dollars.

Yesterday, a civil complaint was filed in Connecticut against 13 "John Doe" defendants, alleging that they engaged in wire fraud, bank fraud, and illegal interception of electronic communications. Search warrants were obtained for the command and control servers in Arizona, Georgia, Texas, Ohio, and California. And a seizure warrant was issued in Connecticut for 29 Internet domain names used by the thieves.

# Mission Afghanistan

## Part 1: Our Role in the War Zone

Night is falling in Afghanistan, and the evening call to prayer can be heard beyond the walls of the U.S. Embassy in Kabul. Inside the compound, our legal attaché is still at work, discussing investigations and other matters by video teleconference with senior executives at FBI Headquarters in Washington, where it is morning some 7,000 miles away. Here in the war zone, on the front lines of the nation's fight against terrorism, fulfilling the Bureau's mission is paramount regardless of the hour.

**Our legal attaché offices—legats—are located in 61 countries around the world, but none are as large as the Afghanistan operation and few are as precariously placed.** With approximately 75 Bureau personnel in the country gathering intelligence, conducting investigations, and mentoring Afghan law enforcement, "We function like a field division in a combat zone," said Legal Attaché Stephen Vogt. "The biggest thing we do here is protect the homeland, and unquestionably, our work has helped save lives."

Because the FBI is known primarily for its domestic law enforcement work, many Americans are surprised to learn just how international the organization has become, particularly since the 9/11 attacks. Today, our investigative and intelligence-gathering expertise play a key role in the war zone, a fact readily acknowledged in the highest U.S. diplomatic and military circles.

Our work in Afghanistan—which began in late 2001—marks the first time the FBI has conducted such operations in a combat zone overseas, beyond some limited efforts during World War II and other brief missions.

During the next several weeks, in articles, photos, and video, FBI.gov will take readers inside Legat Kabul. From a former Russian bunker that houses the Major Crimes Task Force to a forbidding 14,000-foot mountain where our agents helped recover the remains of airplane crash victims, our coverage will highlight the work of the Bureau's dedicated men and women who volunteer for what is often a difficult and dangerous assignment.

**"FBI people who want to make a difference thrive here," explained former Legal Attaché Bob Jones.** Those who volunteer for 120-day assignments—some serve for a year—are among the Bureau's most talented and motivated employees. They willingly sign on for long hours seven days a week, living conditions in

**Kabul as seen from the U.S. Embassy, where our legal attaché coordinates the Bureau's role in the region**

sandbag-reinforced trailers that make college dorm rooms look spacious, and the knowledge that they are a great distance from their loved ones and the normal comforts of home.

But the work—to help safeguard our national security—is extremely rewarding, and hundreds of Bureau personnel volunteer for the war zone. For many, the desire to make a contribution here can be traced back to the events of September 11, 2001.

**"The 9/11 attack against the U.S. was planned in Afghanistan by al Qaeda with the witting support of the Taliban leadership at that time," noted U.S. Ambassador to Afghanistan Karl Eikenberry from his embassy residence in Kabul. "That's why we're here, and we can never forget that. The FBI mission is very central to our efforts," he added. "They're playing a vital role to defeat al Qaeda."**

Special Agent Tom Krall, a New Yorker who now works in our Washington Field Office and has deployed to Afghanistan on several occasions, echoed the ambassador's sentiments. "My first taste of terrorism was on 9/11, standing near the World Trade Center as it came down. I was about a block away. I lost a lot of friends that day," he said, "and I know the attack planning started right here. That's why I volunteer to come to Afghanistan. It's very important we make sure an attack like that doesn't happen again."


Left: The FBI's role on the Major Crimes Task Force is to mentor and train Afghan law enforcement on high-level investigations such as kidnapping, corruption, and organized crime.

# Mission Afghanistan

## Part 2: The Major Crimes Task Force

On a hillside compound just outside Kabul, the Afghan general who leads a new criminal task force is explaining the history of modern policing in his country. Under Soviet rule, he said, the Russians instituted and enforced their own laws. Later, "the Taliban took over and destroyed all of our police force. So our current force is completely new, created from zero, and we have some challenges."

**That's why a little more than a year ago we established the Major Crimes Task Force (MCTF), to build Afghan law enforcement capacity through FBI-led training and mentoring.**

"We help the Afghans with high-level investigations in corruption, kidnapping, and organized crime," said Special Agent Jason Fickett, an assistant legal attaché in Kabul who oversees the MCTF—the largest international task force the FBI has ever operated.

"Prior to us coming here," Fickett said, "one of the biggest challenges the Afghans had is they didn't have the knowledge—the toolkit, so to speak—on how to go about investigating organized crime or putting together comprehensive cases on major players here in the Afghan theater."

That is quickly changing. "Our FBI mentors are working side by side with us inside the task force," said the Afghan colonel who leads the kidnapping unit. Through an interpreter at the MCTF headquarters, housed in a former Russian bunker, he explained, "They share their expertise. They show us new techniques of investigation—putting people under surveillance, how to use wiretaps, how to make arrests. We are very successful because of our mentors."

**"Our agents are mentors in the truest sense of the word," said Fickett. "They don't conduct surveillance or go on arrests. Their role is strictly to teach and to train.** He added, "This is the Afghans' task force. The best way for them to learn is to have them do everything."

The FBI has approximately 15 agents working at the MCTF, but the task force is also represented by veteran law enforcement officers from other U.S. agencies including the Army's Criminal Investigation Division, as well as from Great Britain, France, Canada, and Australia.

In all, about 40 international mentors support nearly 170 Afghans on the task force. All the Afghans—who go through a vetting process before joining the MCTF, which includes a polygraph test—receive basic law enforcement training, and many have taken additional courses at the FBI's training facility in Quantico, Virginia.

**Since the MCTF was formally established in January 2010—with funding from the U.S. Department of Defense—nearly 150 cases have been initiated, "and we've had a number of significant arrests," Fickett said. "Everything is done according to Afghan law."**

"There are challenges," he acknowledged. "It hasn't all been perfect. The government of Afghanistan is trying to work through the rule of law process. And the acceptance of good governance, transparency, and accountability among its public officials is not something that the government is used to."

But good governance is a primary U.S. mission in Afghanistan, and the Bureau's capacity-building efforts through the MCTF are helping to further promote the rule of law and accountability of public officials.

"When you have that accountability," Fickett said, "the safer people feel and the more supportive they're going to be of the government. And the more stable this government is, the better our relationship is going to be with it for many years to come."

# Mission Afghanistan: Contract Corruption

## Part 3: Holding Americans Accountable in a War Zone

The meeting took place at the Serena hotel in Kabul. The senior construction manager made it clear he needed $190,000 in cash to award a U.S.-funded contract to build a school and a hospital in Afghanistan. He didn't realize that the "subcontractor" he was talking to was really one of our undercover agents and that his bribe demand—including the acceptance of a $10,000 good-faith payment—was being recorded on a hidden camera.

**This recent case is one of many investigated by the International Contract Corruption Task Force (ICCTF), whose mission is to go after Americans and others overseas who steal U.S. dollars flowing into the war zone.**

Since Operation Enduring Freedom began in 2002, the U.S. has spent over $770 billion on private contractors who support the military and reconstruction efforts in Afghanistan, Iraq, and Kuwait. With that much money at stake, fraud and corruption are inevitable.

"Most Americans come here to help the people of Afghanistan and believe in the mission," said Special Agent Derek Boucher, who recently completed a yearlong deployment in Kabul working with the ICCTF. "But some of them are taking advantage, and our job is to bring them to justice."

The task force focuses on Americans and other non-Afghans who commit these crimes. "We're not investigating Afghans," Boucher said. "That's the job of the Major Crimes Task Force."

The ICCTF was established in 2006 by a group of U.S. law enforcement agencies and military investigators not only to combat the serious problem of contract corruption in the war zone but to build cases that can be prosecuted in U.S. courts.

The crimes take a variety of forms, including stealing government property such as fuel or other supplies or demanding bribes and kickbacks. A common scheme—like the case above—involves an individual who works for a company that awards U.S. contracts to Afghan construction firms to build roads, hospitals, and schools. The individual might guarantee a $15 million contract to an Afghan subcontractor in return for 10 percent of the contract amount.


**FBI personnel in Afghanistan work long hours, driven in part by the dynamics of working in a war zone.**

**If the payoff occurs, the money lost to fraud could mean that the construction project does not get completed or that it's completed in a substandard way. It might also mean that Afghan subcontractors don't get paid. "The consequences are real," Boucher said.**

ICCTF investigators in Afghanistan rely on tips from the public—similar to how FBI agents may be alerted to fraud at home. But working these cases in a war zone has its own challenges. "The most basic investigative technique is conducting an interview," Boucher said. "Back in the States I go to the person's house or call them into our office. Here, for example, I can't go to an Afghan's house because it might not be safe."

Still, the ICCTF has been successful. Since 2004, the task force has initiated nearly 700 investigations. There are currently more than 100 cases pending in Afghanistan, and since 2007, 37 people have been charged with crimes committed there, and all but one have been convicted, have pled guilty, or are awaiting trial.

"The work the ICCTF is doing is important," Boucher said. "We need to send a message that U.S. taxpayer dollars are going to the Afghan people and not into the pockets of corrupt Americans. Anyone contemplating these types of crimes should know there is no safe haven for them, no matter how far away from home they are."

Left: The fully portable biometrics equipment includes laptop computers and digital fingerprint and retina scanners. As of last November, 300,000 Afghans had been enrolled in the program, from soldiers and police to criminals in prison.

# Mission Afghanistan: Biometrics

## Part 4: A Measure of Progress

The Afghan biometrics program was barely off the ground when it started having an impact.

**Formally established in late 2009 to collect the fingerprints, iris scans, and facial images of Afghan national security forces, the program's initial goal was to keep criminals and Taliban insurgents from infiltrating the army and police force.** But information sharing—with partners like the FBI—is also a key component of the program.

"The FBI has collected thousands of latent prints from the battlefield in Afghanistan," said Special Agent Janeen DiGuiseppi, our liaison officer in Kabul for the biometrics program. "When the Afghans started enrolling people, we began to cross-check our records with theirs."

In fact, when they searched their database, the Afghans identified the 82nd unidentified latent print the FBI passed to them and found that it belonged to an individual they had arrested a few months before as an accessory to a crime. The individual's prints had originally been collected in 2007 in connection with a different crime.

"We were able to give the Afghans information to help them prosecute the case," DiGuiseppi said. "That's exactly the kind of information exchange we are looking for—going both ways. It helps solve crimes, and it enhances security for Afghans and Americans in the war theater."

The biometric program answers two basic questions, said Air Force Lt. Col. Cristiano Marchiori, an advisor to the program: "Who are you, and are you a bad guy?" Already 300,000 Afghans have been enrolled, from soldiers and police to criminals in prison. The ability of the Afghans to collect, store, and match this data against other sources of information is an invaluable tool as the government strives to prevent fraud and corruption.

**The centerpiece of the program is the Afghan Automated Biometric Identification System (AABIS), administered by about 50 Afghans at the Ministry of Interior in Kabul.** The FBI supports the effort through training and mentoring, along with data sharing, said DiGuiseppi. "So far it's been a great partnership. And as the program grows, it will become even more useful."

At the biometrics offices, three shifts of examiners catalog and check fingerprints on large computer screens, while technicians prepare "jump kits"—laptop computers, scanners, and other equipment used in the field to collect fingerprints, facial images, and iris scans. The Afghan colonel who supervises the program emphasized that Afghans are doing all the collections and maintaining the database, but he readily acknowledged the FBI's role in the program. "We are very thankful for the FBI's help and their willingness to train and assist us," he said.

The partnership is mutually beneficial. "A strong Afghan biometric program reduces the enemy's anonymity and his capability to operate anonymously in the battle space," said Marchiori. "If we have one unique identifier—a set of prints, an iris scan—it's hard for the enemy to hide among the population when he's trying to register a vehicle or vote or move around the country freely."

Afghan Ministry of Interior officials plan to use the biometrics program to enroll eight million citizens as part of a national ID effort. "This is for the betterment of the country," one Afghan official said. "This is for security and for helping the Afghan people."

# Most Wanted Terrorist Dead

## Bin Laden Killed in 'Targeted Operation'

The mastermind of the attacks on September 11, 2001 that killed thousands of innocent men, women, and children has been killed.

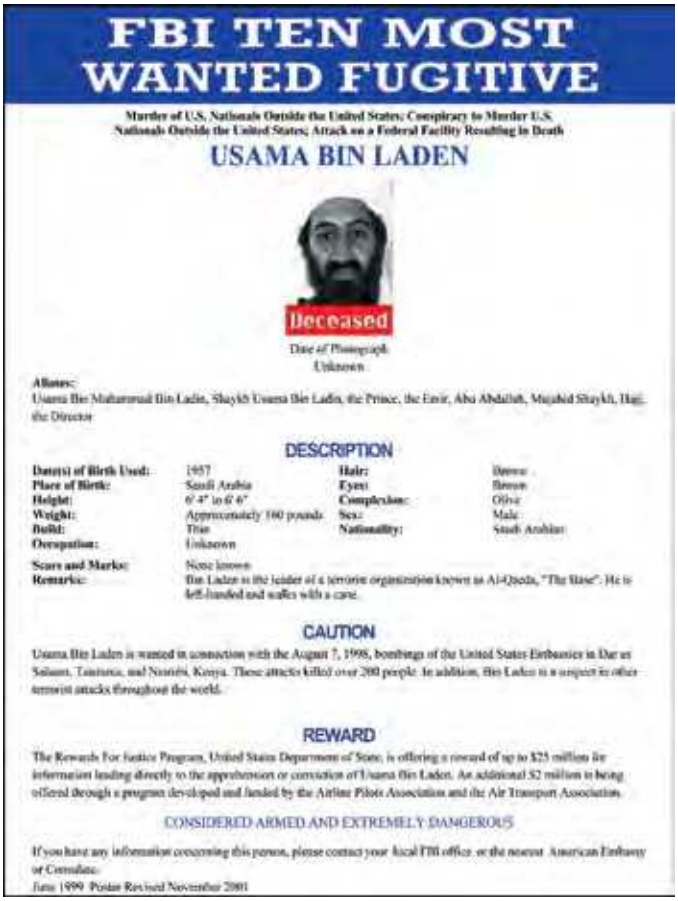
President Barack Obama made the announcement late Sunday evening, May 1, in a televised address to the world. He said he had been briefed by the intelligence community last August that bin Laden was in hiding "within a compound deep inside of Pakistan." Over the intervening months, intelligence agencies worked to confirm the intelligence. Then last week, President Obama determined there was enough intelligence to take action.

**"Today, at my direction, the United States launched a targeted operation against that compound in Abbottabad, Pakistan," the President said from the East Room of the White House. "A small team of Americans carried out the operation with extraordinary courage and capability. No Americans were harmed. They took care to avoid civilian casualties. After a firefight, they killed Osama bin Laden and took custody of his body."**

Well before the events of 9/11, bin Laden had openly declared war on the U.S. and was committed to killing innocents. His al Qaeda group was responsible for the 1998 bombings of the U.S. Embassies in Dar es Salaam, Tanzania and Nairobi, Kenya. The attacks killed over 200 people. Bin Laden was indicted for his role in planning the attacks and added to the FBI's Ten Most Wanted Fugitives list in 1999.

Intelligence agencies quickly learned that the 9/11 attacks were carried out by bin Laden's terrorist organization, and in October 2001, his name was added to the U.S. Department of State's Most Wanted Terrorists List.

"Tonight, we give thanks to the countless intelligence and counterterrorism professionals who've worked tirelessly to achieve this outcome," President Obama said. "The American people do not see their work, nor know their names. But tonight, they feel the satisfaction of their work and the result of their pursuit of justice."


FBI TEN MOST WANTED FUGITIVE

Murder of U.S. Nationals Outside the United States; Conspiracy to Murder U.S. Nationals Outside the United States; Attack on a Federal Facility Resulting in Death

USAMA BIN LADEN

Deceased

Date of Photograph: Unknown

Aliases:

DESCRIPTION

Date(s) of Birth Used: 1957
Place of Birth: Saudi Arabia
Height: 6' 4" to 6' 6"
Weight: Approximately 160 pounds
Build: Thin
Occupation: Unknown
Hair:
Eyes:
Complexion:
Sex: Male
Nationality: Saudi Arabian

Scars and Marks: None known

CAUTION

REWARD

CONSIDERED ARMED AND EXTREMELY DANGEROUS

**Bin Laden was on the FBI Ten Most Wanted Fugitives list as well as the State Department's Most Wanted Terrorists list.**

# Behavioral Interview Program

## Attempting to Understand Violent Offenders

The inmate's wrist and leg shackles were removed and he was led into a small conference room to meet two special agents from our Behavioral Analysis Unit (BAU). The agents were there to conduct an interview into every aspect of the inmate's life—from his earliest childhood experiences to the abduction, sexual assault, and murder of a preteen girl that sent him to prison for life without the possibility of parole.

**Such interviews are part of an ongoing BAU program to understand the minds of violent offenders.** The offender interview program is in keeping with BAU's overall mission to provide behavioral-based support to federal, state, local, and international law enforcement agencies investigating time-sensitive crimes such as kidnappings and other violent offenses.

"We are never going to get the full and complete truth from offenders," said one of the agents who conducted the interview. "But we gather all the information, the truth and the lies, and we learn from both."

The insights from these consensual interviews are used for research and training, and they also have the potential to help investigators in the field. "The next time BAU responds to a child kidnapping case and a young person's life is at stake," the agent explained, "we can say, 'we sat across from a guy who did something similar, and here's what he told us.' "

Behavioral analysts have been popularized in television and movies as expert "profilers," capable of comprehending and even anticipating the thoughts and actions of the worst criminal minds. In real life, the expertise acquired by BAU personnel takes years of training and investigative experience. Offender interviews are an invaluable part of that process.

**"These are not investigative interviews to collect evidence or to determine guilt or innocence," said one of the agents. "We already know the 'how' of the crime. Now we want to know 'why.' "**

Sitting in the small conference room across from the 31-year-old offender, the agents explained the ground rules. "There will be no tricks and no games," they said. "We are going to talk about your life, including the murder. We want to know how you think about things and how you see things."

There is nothing confrontational about the videotaped interview, which lasted for six hours. The offender—who consented to the meeting as part of a plea agreement to avoid the death penalty—talked openly, but perhaps not always truthfully.

"What they choose to share and disclose and what they choose not to disclose can be very revealing," one of the agents said. "Sometimes it is difficult for them to face what they have done and to speak about it out loud."

"From a behavioral standpoint," the other agent said later, "we got a lot out of the interview." Videotaped segments will be used by BAU staff when they train researchers, social workers, medical staff, and law enforcement personnel around the country about offenders who commit violent crimes against children.

"When you can illustrate a point by showing a video clip of the offender in his own words," the agent said, "it is a very compelling teaching tool."

# National Police Week 2011

## Honoring Those Who Serve

Thousands of people gathered today in front of the National Law Enforcement Officers Memorial in Washington, D.C. to honor those who gave their lives in the line of duty. The candlelight vigil included a reading of the 316 names being added to the memorial this year.

In a podcast, Special Agent Jeff Blanton of the FBI's Office of Law Enforcement Coordination discusses National Police Week. " It is truly is a fraternity, it's a brotherhood in law enforcement," Blanton says.

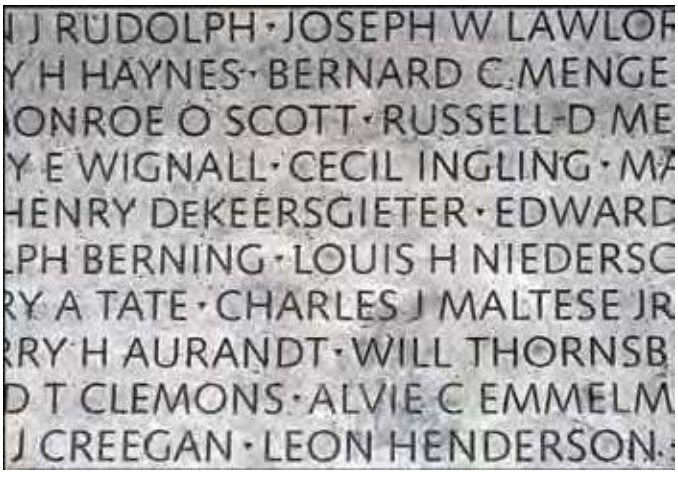
In a video message released May 12, Director Robert S. Mueller said, "On behalf of the men and women of the FBI, I want to personally recognize and thank each of you individually, and all of your departments collectively, as we work together to keep our neighborhoods safe."

In 1962, President John F. Kennedy issued a proclamation designating May 15 as Peace Officers Memorial Day and the week in which it falls as Police Week. Today, law enforcement officers from around the world attend events in Washington, D.C. to honor colleagues who have made the ultimate sacrifice.

**Fifty-six law enforcement officers were feloniously killed in the line of duty during 2010, according to statistics released by the FBI in May. By region, 22 victims were killed in the South, 18 in the West, 10 in the Midwest, three in the Northeast, and three in Puerto Rico. The total number of officers feloniously killed in 2010 was eight more than the 48 officers slain in 2009.**

**Thousands of people attended a candlight vigil at the National Law Enforcement Officers Memorial in Washington, D.C.**

**Representative Steny H. Hoyer, left, and FBI Director Robert S. Mueller at the candlelight vigil**




**The National Law Enforcement Officers Memorial wall**

# Child Predators

## The Online Threat Continues to Grow

It's a recipe for trouble: naive teenagers, predatory adults, and a medium—the Internet—that easily connects them.

**"It's an unfortunate fact of life that pedophiles are everywhere online," said Special Agent Greg Wing, who supervises a cyber squad in our Chicago Field Office.**

When a young person visits an online forum for a popular teen singer or actor, Wing said, "Parents can be reasonably certain that online predators will be there." It is believed that more than half a million pedophiles are online every day.

Agents assigned to our Innocent Images National Initiative are working hard to catch these child predators and to alert teens and parents about the dark side of the Internet—particularly when it comes to social networking sites and, increasingly, online gaming forums.

Pedophiles go where children are. Before the Internet, that meant places such as amusement parks and zoos. Today, the virtual world makes it alarmingly simple for pedophiles—often pretending to be teens themselves—to make contact with young people.

Even without being someone's "friend" online, which allows access to one's social networking space, pedophiles can see a trove of teenagers' personal information—the town they live in, the high school they attend, their favorite music and TV programs—because the youngsters often post it for anyone to see.

"The younger generation wants to express themselves, and they don't realize how vulnerable it makes them," Wing said.

**For a pedophile, that personal information is like gold and can be used to establish a connection and gain a child's trust.**

There are basically two types of pedophiles on the Internet—those who seek face-to-face meetings with children and those who are content to anonymously collect and trade child pornography images.

Those seeking face-to-face meetings create bogus identities online, sometimes posing as teenagers. Then they troll the Internet for easy victims—youngsters with low self-esteem, problems with their parents, or a shortage of money. The pedophile might find a 14-year-old girl, for example, who has posted seemingly harmless information on her space for anyone to see. The pedophile sends a message saying he goes to high school in a nearby town and likes the same music or TV shows she likes.

Then the pedophile cultivates a friendly online relationship that investigators call "grooming." It could continue for days or weeks before the pedophile begins bringing up sexual topics, asking for explicit pictures or for a personal meeting. By that time an emotional connection has been made—and pedophiles can be master manipulators. Even if an actual meeting never takes place, it is important to note that youngsters can be victimized by such sexually explicit online contact.

**Even worse than posting personal information for anyone to see is the fact that many youngsters will accept "friends" who are total strangers.** "Nobody wants to just have five friends online," Wing said. "It's a popularity thing."

Special Agent Wesley Tagtmeyer, a veteran cyber investigator in our Chicago office who works undercover during online investigations, said that in his experience, about 70 percent of youngsters will accept "friend" requests regardless of whether they know the requester.

Tagtmeyer and other cyber investigators say a relatively new trend among pedophiles is to begin grooming youngsters through online gaming forums, some of which allow two-way voice and video communication. Parents who might be vigilant about monitoring their children's Internet activity often have no idea that online video gaming platforms can pose a threat.

"Parents need to talk to their children about these issues," he said. "It's no longer enough to keep computers in an open area of the house so they can be monitored. The same thing needs to be done with online gaming platforms."

# Mission Afghanistan: Pamir Air Crash

## Part 5: Humanitarian Effort in the War Zone

Pamir Airways Flight 112 left Kunduz Province in Afghanistan last May bound for Kabul with 44 people aboard. About 25 miles from its destination, in heavy wind and dense fog, the plane crashed into a mountain in the remote Hindu Kush nearly 14,000 feet above sea level. No one survived.

**The crew and passengers were mostly Afghan, but the dead also included citizens of Turkey, Great Britain, the Philippines, and the U.S.** Because of the one American victim, our legal attaché in Kabul was asked to assist the Afghan government with recovering and identifying the bodies, a task that would prove as grim as it was difficult.

The crash site, in such an inaccessible location and at such a high elevation, could only be safely approached on foot, and then only after the weather improved. When teams were finally able to reach the site, they were met with a horrific scene, and what began as a recovery operation soon turned into an extraordinary humanitarian effort to identify the victims and repatriate their remains—and to bring some relief to the victims' loved ones.

"Just hiking to the foothill of the crash site was a challenge, and then you're looking straight up at this big slide of debris," said Special Agent Adriene Sullivan, a 14-year FBI veteran.

"You are going up this ravine and everything is loose rock," she said. "If you lose your footing, you're going all the way down." Wearing an armored-plated vest and carrying a weapon—even at that elevation the Taliban was still a threat—Sullivan recalled, "I just had to take a deep breath and go up the mountain. It was tough."

**Dealing with the crash site was even tougher.** The plane was estimated to be traveling at 250 mph when it slammed into the mountainside. The impact was so violent that passengers' bodies could not be identified.

"There was not a lot to go on," Sullivan said. "Bodies were unrecognizable, and nothing was on them like a wallet in someone's back pocket."

**Pamir Airways Flight 112 crashed last May in the mountains outside Kabul, killing 44 people, including one American. Our legal attaché was asked to assist in effort to recover and identify the bodies.**

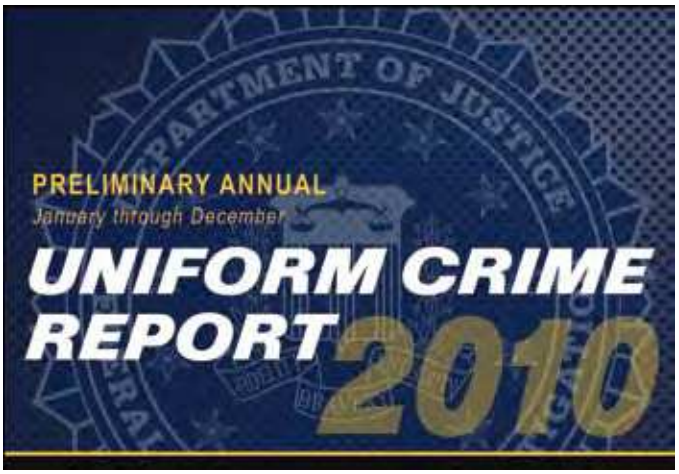
Agents and other Bureau personnel worked with the Afghan military and international partners to retrieve 180 bone and tissue samples, which were transported to the Afghan National Army morgue in Kabul. There, Turkish and British disaster victim identification teams conducted sophisticated deep tissue and bone DNA samples, using expertise unavailable to the Afghans or our agents overseas.

**"We learned a lot about that type of DNA sampling and so did the Afghans," Sullivan said.** The samples were sent to Turkey and England, and remarkably, all 44 individuals were identified.

Months after the crash—which was ruled a weather-related accident—a ceremony was held in Kabul so family members could bury their loved ones.

"It was very satisfying that we were able to help the families," said Sullivan, who volunteered for a year-long assignment in the war zone. "Everybody worked together incredibly well, and the Afghans were extremely grateful for our help."

This wasn't a typical mission for our people on the front lines of the fight against terrorism, but it was an important one, and it forged lasting relationships with the Afghans and our international partners.




# Crimes Rates Fall Again

## According to Preliminary Stats

Preliminary FBI figures reveal that the levels of both violent crime and property crime in the U.S. declined in 2010 from the previous year's data.

The 2010 *Preliminary Annual Uniform Crime Report*, just released today, shows a 5.5 percent decrease in the number of reported violent crimes when compared with data from 2009. It also shows a 2.8 percent decline in reported property crimes.

This latest report is based on information submitted to the FBI from 13,007 law enforcement agencies around the country. The crimes covered are murder, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson.

**Some of the report's highlights include:**

- Nationally, murder declined 4.4 percent, while forcible rape dropped 4.2 percent, robbery 9.5 percent, and aggravated assault 3.6 percent—all when compared with 2009 crime figures.
- Geographically speaking, the South saw the largest decline in violent crime (7.5 percent), followed by the Midwest (5.9 percent), the West (5.8 percent), and the Northeast (0.4 percent).
- Concerning property crime, motor vehicle theft was down 7.2 percent, larceny-theft was down 2.8 percent, and burglary was down 1.1 percent. Arson, tracked separately from other property crimes, fell 8.3 percent nationally.
- All regions of the country experienced overall declines in property crime during 2010 from 2009 rates: down 3.8 percent in the South, 2.7 percent in the Midwest, 2.5 percent in the West, and 0.5 percent in the Northeast.
- All city population groups saw decreases in violent crime.
- Cities with populations of less than 10,000 saw a significant drop in murder—a 25.2 percent decrease.

**There were some specific increases noted:**

- The Northeast saw increases in some violent crime categories from 2009 figures—murder was up 8.3 percent, forcible rape up 1.4 percent, and aggravated assault up 0.7 percent.
- Cities with populations of 250,000 to 499,999 saw a 3.0 percent rise in murder, while cities with populations of 500,000 to 999,999 saw a 1.9 percent increase in forcible rape, and cities between 25,000 and 49,999 saw an increase of 1.3 percent in burglary.
- The Northeast also saw an increase in burglary—up 3.5 percent.
- Non-metropolitan counties reported slight increases in burglary (1.2 percent) and larceny-theft (3.2 percent).

Also available in the preliminary report are tables that include the number of offenses reported by cities—organized by state—with populations of more than 100,000. These tables include preliminary totals of offenses known to law enforcement for agencies that provided us with 12 months of complete data in both 2009 and 2010.

As always, we caution against drawing conclusions from the data in this report by making direct comparisons between cities. Valid assessments are possible **only** with careful study and analysis of the range of unique conditions affecting each local law enforcement jurisdiction.

Complete figures for 2010 will be released this fall in the full *Crime in the United States* report.

# Mafia Takedown

## Philadelphia Boss Charged

On Monday, a superseding federal grand jury indictment was announced charging 13 members and associates of the Philadelphia La Cosa Nostra (LCN) family with racketeering, extortion, loan sharking, illegal gambling, and witness tampering.

Eleven of the 13—including the reputed boss and underboss of the criminal enterprise—were arrested earlier that day in Philadelphia and New Jersey. Two of the subjects were already serving time in federal prison for previous convictions but managed to continue their racketeering activities from behind bars.

Alleged mob boss Joseph Ligambi rose through the ranks of the Philadelphia LCN crime family and took over at the helm after the 2001 incarceration of previous boss Joseph "Skinny Joey" Merlino on racketeering charges.

**The indictment alleges that for more than a decade, Ligambi, underboss Joseph Massimino, and the others conspired to generate money through various crimes.** For example, they reportedly operated illegal gambling businesses involving sports bookmaking and electronic gambling devices in places like bars, restaurants, convenience stories, and coffee shops…and pocketed the proceeds. Mafia families like the one in Philadelphia often make millions of dollars and traditionally use gambling proceeds as seed money for other crimes.

The defendants also offered "loans"—at exorbitant interest rates—to victims who knew there would be dire consequences if they failed to repay them within a certain time frame.

**To carry out their crimes, the defendants often used actual or implied threats of violence against their victims.** According to the indictment, some of the defendants used phrases like, "I'll put a bullet in your head," and, "Chop him up," to threaten victims who weren't repaying their loans. The defendants used their reputation for violence to intimidate and prevent victims and witnesses from cooperating with law enforcement.

**The defendants also actively worked to conceal their illegal operations from law enforcement.** For example, they used coded language over the phone, such as calling the electronic gambling devices "coffee machines." They often took "walk and talks" where they would conduct covert conversations with each other while walking to and from a particular destination because they thought they couldn't be intercepted. They also established companies that appeared to be legitimate but were actually created to launder money and conceal the illegal nature of their activities.

**Philadelphia Special Agent in Charge George Venizelos, at podium, announces indictments.**

To collect the evidence needed for these indictments, this long-term investigation included undercover scenarios, court-authorized electronic surveillances, consensual recordings, and many hours of physical surveillance.

**This particular case was a good example of law enforcement cooperation at its best**—the Philadelphia Police Department, the Pennsylvania and New Jersey State Police, the Criminal Division of the Internal Revenue Service, and the Department of Labor all worked alongside the Philadelphia FBI, with additional assistance from the New Jersey Department of Corrections and the Pennsylvania Attorney General's Office. Prosecutors from the Pennsylvania Attorney General's Office and the Department of Justice's Organized Crime and Racketeering Section are assisting the U.S. Attorney's Office in the Eastern District of Pennsylvania as well.

This arrest of the reputed leadership of the Philadelphia LCN comes on the heels of the large mafia takedown in New York earlier this year. And law enforcement efforts against the LCN, as well as other types of organized crime—international and domestic—will continue unabated.


Left: At the U.S. Embassy in Kabul, FBI intelligence analysts work in a space dubbed "the bullpen."

# Mission Afghanistan: Analysts in the War Zone

## Part 6: Turning Information Into Intelligence

Intelligence analyst Courtney C. had been in Afghanistan only a few days when she saw firsthand the value of her work in the war zone.

**"We got a report from the military that a person of interest had been picked up in one of the provinces," said Courtney, who joined the Bureau five years ago.** Information was needed about the individual's possible connection to terrorist activity, but the only thing to go on was a passport number and a few personal items he had with him.

In a matter of hours, using law enforcement and military records and additional resources, she and others were able to collect and analyze a range of information and provide investigators with a more complete picture of the man's identity—including a pattern of what seemed to be suspicious activity related to the movement of money.

Gathering and analyzing information—whether about a terrorist threat or a criminal enterprise—is exactly what intelligence analysts do every day across the FBI's many investigative programs. But in the war zone, there is often a greater sense of urgency because lives can hang in the balance.

**"Everything's a lot more immediate here," said Courtney, who is based in one of our Midwest offices but recently began a four-month assignment in Kabul. "You need to push things out a lot quicker, because there are real-time implications if you don't."** The timely dissemination of intelligence, for example, can have an immediate impact on the safety of troops on the ground.

The FBI's top investigative priority is to protect the homeland from terrorist attack. The ability to collect intelligence in the war zone—in a cooperative effort with our U.S., Afghan, and other international partners—is critical for our domestic security as well as keeping our people on the front lines safe. Intelligence analysts play a critical part in that process.

**"We are information brokers," Courtney said. "Our role is to take information and give it context. The intelligence we gather from a variety of sources is pushed out to investigators in the field and to our partners, where it can be integrated into operations."**

In Afghanistan, just like at home, intelligence comes from many places—open sources like newspapers and the Internet, military and law enforcement databases, and citizens providing tips, to name a few.

When it comes to counterterrorism matters, the cycle of collecting, analyzing, and sharing intelligence is intensified and compressed. "In the war zone, we are at the razor's edge of knowledge creation as it relates to a lot of terror threats," Courtney said. "Information we collect here today could save lives on the front lines and at home. Knowing that makes everyone work that much harder."

Beyond the intense pace—"No two days are the same here," she said—there is also the satisfaction of working with a dedicated group of people who care deeply about the FBI's mission in the war zone.

"Most of us are here for four months," she explained. "It's 120 days to make a difference and to contribute. I see it as a once-in-a-lifetime opportunity."

# Digital Forensics

## Regional Labs Help Solve Local Crimes

In 2008, Illinois police received disturbing information about a Chicago woman who had taken a 3-year-old to a "sex party" in Indiana where the child and an 11-year-old girl were abused by three adults. However, by the time the tip was received, the crime had already occurred, and there seemed to be no evidence to support criminal charges.

**But there *was* evidence, buried deep within the woman's computer, and examiners from our Regional Computer Forensics Laboratory (RCFL) in Chicago found it—a deleted e-mail titled "map to the party" that contained directions to an Indiana hotel.** The evidence led to charges against all three adults, who were later convicted of aggravated sexual abuse and are currently in prison serving life sentences.

"That's just one example of what we do every day," said John Dziedzic, a Cook County Sheriff's Office forensic examiner who is the director of the Chicago RCFL. "Evidence we produce here—and testify to in court—is crucial in a variety of major investigations."

The FBI established the first RCFL in San Diego in 2000, and today there are 16 Bureau-sponsored labs located around the country, staffed by agents and other federal, state, and local law enforcement agencies.

Each facility is a full-service forensics laboratory and training center devoted to examining digital evidence in support of investigations—everything from child pornography and terrorism to violent crime and economic espionage cases.

**Using sophisticated tools and technology, RCFLs analyze evidence from all kinds of electronic devices, including computers, cell phones, video game consoles, and even reel-to-reel tapes.**

"Anything that can store data electronically can be analyzed," said Special Agent Justin Poirier, deputy director of the Chicago RCFL.

RCFL examiners—all certified by the FBI—specialize in locating encrypted, deleted, or damaged file information that could be used as evidence in an investigation.

"Digital evidence has become part of just about every type of investigation," Poirier said, "because today everybody uses computers and portable electronics such as cell phones."


**RCFL examiners—all certified by the FBI—specialize in locating encrypted, deleted, or damaged file information that could be used as evidence in an investigation.**

**The benefit of having a regional forensic facility, he added, is that the FBI can bring its expertise and training directly to where it is needed.**

"The idea is to create regional resources," Poirier explained. "We train the state and local examiners, who make a three-year commitment to the RCFL. When they return to their agencies, they have expertise and access they didn't have before. And in the process, we build lasting relationships with our regional partners."

Dziedzic added, "Instead of sending evidence to the FBI Laboratory in Quantico, we can analyze it much faster here in our own backyard."

Chicago's RCFL was established in 2003 and consists of five FBI employees and 13 examiners from agencies including the Chicago Police Department, Cook County Sheriff's Office, and U.S. Customs and Border Protection. It is the only digital forensics lab in Illinois to be accredited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board.

"Accreditation is the gold standard when it comes to prosecuting cases and testifying in court," Dziedzic said. "It means that we operate at the highest professional standards."

"Criminals are using more sophisticated electronic methods to commit crimes," Poirier said. "This regional approach to digital forensics—pairing the Bureau with local law enforcement to collaborate on cases—is the future for law enforcement. It really works."

Left: A special agent's protective vest attests to the dangers of operating in a war zone. The U.S. military tapped the FBI's expertise for a variety of uses, including helping to disrupt and stop deadly suicide bomb attacks.

# Mission Afghanistan: Legat Kabul

## Part 7: An Early Presence in the War Zone

The FBI's presence in Afghanistan began in 2001 with a handful of agents whose job was to search for information regarding terror threats to the homeland. By the time our legal attaché office, or legat, was formally established in 2006, dozens of Bureau personnel were involved in a range of investigative and intelligence-gathering activities to support the U.S. mission in Afghanistan.

**Ordinarily, the FBI's 61 international offices serve mainly as law enforcement liaisons with their host countries, but Legat Kabul has taken on a much broader role.**

"Things are different in a war zone," said Special Agent Brian McCauley, the first legal attaché in Afghanistan. "We couldn't just be a liaison service in Afghanistan because the mission required a greater contribution. When the military and others realized what our capabilities were and the value that we added," he said, "we began to do much more."

Over time, in addition to counterterrorism work, Bureau personnel began providing law enforcement training and mentoring to Afghans, helping them build a government based on the rule of law. And our investigative and intelligence-gathering expertise was tapped by the military for a variety of uses, including helping to disrupt and stop deadly suicide bomb attacks.

**"The army is not raised and trained to gather and analyze intelligence from the battlefield the same way the FBI is," said Major Gen. Bernard Champoux, commander of the Army's 25th Infantry Division who formerly served as deputy chief of staff for operations for NATO forces in Afghanistan.** "The FBI brings a skill set that is not found in other organizations," he said. "The level of professionalism, training, and sense of mission that you find in the FBI is extremely admirable."

"In the early days," McCauley said, "the challenge was defining the FBI's mission, to see where we could add value. And once we did define and expand our mission," he added, "we had to fully support it." That meant proper training for Bureau personnel who deployed and the significant logistical task of providing housing, equipment, and supplies for those who would be working in a hostile and austere environment some 7,000 miles from home.

One reason the FBI has adapted so well in the war zone, Gen. Champoux believes, is the Bureau's team approach. "The FBI is accustomed to working with its law enforcement partners in task force settings—which is exactly the way the coalition forces' counterinsurgency operation works. You are part of a team, and you have to play well together."


Major Gen. Bernard Champoux

McCauley is particularly proud of the team effort that targeted improvised explosive device (IED) cells. During his deployment, the Bureau helped dismantle four IED cells and stop 43 separate attacks.

**"The FBI knows how to conduct investigations and interviews—we've been doing this for over 100 years," McCauley said.** "An IED cell is really just another type of organized crime. There are leaders, recruiters, facilitators, bomb makers, and the sacrificial volunteers who carry out attacks. Our investigative and intelligence-gathering approach helped alter events and prevent attacks. Without question, our joint efforts with the military and other partners saved countless lives."

Gen. Champoux noted that McCauley's "willingness to find a way to make a contribution and to bring the FBI's capability forward made a huge difference in the success of our operations against IEDs." He added, "The FBI has been a great partner to the military in Afghanistan."

# Mission Afghanistan: A Model for the Future

## Part 8: Legat Kabul and the International Fusion Cell

From the roof of the U.S. Embassy in Kabul, Legal Attaché Bob Jones surveyed a city ravaged by decades of war and reflected on the FBI's role on the front lines in the fight against terrorism.

**"The biggest thing we do here is protect the homeland from afar," said Jones, who recently completed a 15-month assignment as the FBI's senior official in Afghanistan.**

U.S. Ambassador to Afghanistan Karl Eikenberry amplified Jones' comments. "The FBI is the shield in the United States," he said. "But what 9/11 taught us is that you can't defend the country against terrorism from the U.S. shoreline. You must extend the shield globally and integrate it with other international crime-fighting and counterterrorist organizations. The FBI," he added, "plays a unique and important role in the combined approach that we use on the ground in Afghanistan."

Counterterrorism may be the Bureau's most important responsibility in the war zone, but it is not our only responsibility. The mission in Afghanistan—and elsewhere around the world—includes protecting U.S. interests abroad from criminal threats well as those related to terrorism. To accomplish this, Legat Kabul prioritizes several key areas of operations: information sharing, specialized investigations, and a small but influential role in capacity building.

"Capacity building is essentially helping the Afghans build their law enforcement expertise," Jones said. "They've already got a robust investigative capacity inside the Ministry of Interior and the National Directorate of Security. But through the Major Crimes Task Force and other Bureau initiatives, we can help make them better."

Some of those other capacity-building initiatives include assisting the Afghans with their expanding biometrics program and providing law enforcement leadership training, both on the ground in Afghanistan and at our training facility in the U.S.

Collecting information and intelligence—another critical priority—has always been a hallmark of the FBI, Jones said, "and since 9/11, we have expanded that ability.

**The FBI mission in Afghanistan—and elsewhere around the world—includes protecting U.S. interests abroad from criminal threats as well as those related to terrorism.**

Today, we are a true partner in the inter-agency community when it comes to collecting, processing, and sharing intelligence. That intelligence-driven approach," he added, "helps save lives."

**"Afghanistan is a tough environment to operate in," Jones said. "It's an active war zone with an active insurgency, and that brings a particular set of challenges."**

To help manage those challenges, FBI Director Robert S. Mueller created the International Fusion Cell (IFC) in 2008 within our International Operations Division to provide support and guidance to FBI operations in Iraq and Afghanistan. The IFC, largely staffed by Bureau personnel who are veterans of multiple war zone deployments, provides oversight and leadership to Legat Kabul.

Jones and others believe the hard-won skills gained in Afghanistan—along with our previous experience in Iraq and other international locations—will pay dividends when we respond to future war zones.

"The IFC has created an excellent model for legat operations in conflict zones," said recently retired Special Agent Ed Montooth, who managed the fusion cell. "The processes we have developed based on our experiences and lessons learned in Iraq and Afghanistan will make us much more effective going forward," he added.

"Whether it's Afghanistan or elsewhere," Montooth explained, "we now have a successful and tested model—both at FBI Headquarters and in the legats—to address these unconventional situations that have significant national security implications."

Left: In 1995, four of poet Walt Whitman's 10 missing notebooks were recovered when they turned up at auction. The rest are still missing.

# National Treasures

## Recovering Artwork Owned by the U.S. Government

In 1942, with World War II raging, the Library of Congress took the precaution of sending some of its national treasures to a guarded facility in the Midwest, including a collection of Walt Whitman's papers, which were sealed in packing cases prior to shipping. When the collection was returned to Washington in October 1944 and unsealed, 10 of the illustrious poet's notebooks were missing.

**The library searched for the notebooks—and enlisted the FBI's help—but to no avail. It was eventually concluded that the missing items were intentionally removed before they were shipped in 1942.** More than five decades later, in 1995, four of the notebooks were recovered when they turned up for sale at Sotheby's, but six of the priceless artifacts are still unaccounted for.

The Whitman notebooks are perhaps the most intriguing example of a little-known phenomenon in the world of art investigations: items owned by the U.S. government that have gone missing, many dating back to the New Deal era of the 1930s.

"Trying to locate items that disappeared decades ago represents a significant challenge for law enforcement," said Bonnie Magness-Gardiner, who heads the FBI's art crime team. "But we are bringing modern technology to the effort with our new National Stolen Art File, and we are seeing results."

The National Stolen Art File (NSAF) is an online database of stolen art and cultural property reported by law enforcement agencies throughout the United States and the world and maintained by the FBI. It consists of images and physical descriptions of thousands of stolen and recovered objects in addition to investigative case information. The database is a resource for art crime investigators and for gallery owners, dealers, and auction houses seeking to authenticate works and verify ownership. The public can also search the free online tool, minus the investigative information.

In partnership with other agencies such as the Library of Congress and the General Services Administration (GSA), which is responsible for artifacts and artworks in federal facilities, the FBI uses the NSAF to locate and recover missing artworks owned by the government.

As the official custodian of artworks produced under the federal Works Progress Administration (WPA) during the New Deal era, the GSA has partnered with the FBI and the art community to recover misplaced and stolen WPA works. The agency maintains an inventory of significant WPA art, which has been added to the FBI's database.

**"Often the people in possession of these WPA works don't realize they have no legitimate claim on them," said Gardiner. "They may have inherited them or found them in the attic of their grandparents' house."** In an attempt to value or sell the works, the possessors contact dealers or auction houses, who, in turn, consult the NSAF and discover the items are rightfully owned by the government.

Investigators with the GSA's Office of Inspector General work to authenticate and recover the works, and in many cases, the agency then loans the recovered items to museums and galleries across the nation, where they can be enjoyed by the public—as they were intended to be.

"These works commissioned in the 1930s and '40s are part of America's culture and history," Gardiner said. "They belong to the government, but really they belong to the public, and we are working to make sure that the public has access to them."

# Biometric Sharing Initiative

## Making the World Safer

Known or suspected terrorists. Transnational criminals. Both threaten not only U.S. security but the security of nations around the world.

One way to help reduce this threat is for nations to share fingerprints and other kinds of biometric information on terrorist-related subjects and international criminals who've had previous brushes with law enforcement. Here in the U.S., the FBI's Criminal Justice Information Services Division—through its Foreign Biometric Exchange program—serves as the centralized collection point for foreign fingerprint records and other biometric data.

Actually, the Bureau has been exchanging fingerprints internationally for nearly 80 years, primarily in criminal matters. But after the terrorist attacks of 9/11, the U.S. Attorney General specifically directed the FBI to obtain and maintain fingerprints and other biometrics for known and suspected terrorists processed by foreign law enforcement agencies. We then expanded the initiative to include international criminals, who, like terrorists, routinely cross national borders to commit their crimes and often use aliases.

**The Foreign Biometric Exchange program is coordinated by CJIS's Global Initiatives Unit.** Says Gary Wheeler, who heads up the unit, "Our mission is two-fold—in addition to collecting and analyzing the data we receive, we also offer assistance to nations who want to develop their own automated biometric systems that meet international standards." To accomplish both tasks, unit personnel work with our International Operations Division at FBI headquarters, our legal attaché officers overseas, and sometimes INTERPOL and other U.S. federal agencies.

**How it all works:** If a nation is interested in participating, we first assess its fingerprint capabilities through surveys and on-site visits. Then we determine what, if any, assistance we can provide in terms of equipment—like mobile fingerprint devices—and training in areas like basic fingerprinting and identification, crime scene preservation, and latent print collection.

Once we begin receiving data from a global partner—either in batches or on a case-by-case basis—we run their fingerprints (both known and unknown) against our

**The FBI's Integrated Automated Fingerprint Identification System contains records of approximately 67 million criminal subjects, including known or suspected terrorists, military detainees, and international criminals.**

Integrated Automated Fingerprint Identification System (IAFIS). Currently, IAFIS contains records of approximately 67 million criminal subjects, including known or suspected terrorists, military detainees, and international criminals.

If there's a match in IAFIS, we notify the submitting nation. If there's no match, a new IAFIS record can be created and included in future searches requested by international, national, and perhaps most importantly, local law enforcement officers who are our first line of defense against threats to public safety.

Since 2002, the Global Initiatives Unit has developed relationships with more than 50 countries and has received over 450,000 biometric records that have been added to IAFIS.

Left: A sawed-off shotgun is uncovered during a search by the Violent Crimes Task Force, which is made up of Chicago Police Department officers, Cook County Sheriff's Office deputies, and FBI agents.

# Chicago's Violent Crime Fighters

## Partnerships Key to Task Force Success

As a chilly spring drizzle fell in one of Chicago's most dangerous neighborhoods, FBI agents and Chicago Police Department officers on our Violent Crimes Task Force gathered on a rooftop parking garage for a last-minute briefing before executing a search warrant nearby involving a recently paroled felon.

**Members of the task force donned bullet-proof vests and finalized their operational plan. The felon in question was believed to be violating his parole by carrying a sawed-off shotgun, and every safety precaution needed to be taken.**

Established in 1989, Chicago's Violent Crimes Task Force is one of the oldest continuing task force operations in the FBI. The squad, known as VC1, consists of agents and members of the Chicago Police Department (CPD) and Cook County Sheriff's Office who work side by side and are on call around the clock.

"If something happens," said Special Agent Mark Quinn, who joined the squad in 1994 and has supervised it since 2006, "we respond. Our first priority is public safety."

The task force handles a variety of violent crimes such as extortion and murder for hire, but the "big three" offenses it investigates are kidnappings, bank robberies, and fugitive matters.

VC1 is staffed by seasoned investigators like Quinn and CPD's Sgt. Warren Richards—who was leading the search warrant operation—and young agents learning the ropes and getting valuable street experience.

Special Agent Joe Raschke, an 11-year veteran of the squad, remembers that when he first came to the Chicago Field Office, "VC1 was the squad to be on."

"As a young agent you get great experience," Raschke said, "not just making arrests but interviewing subjects and victims and learning how to deal with a variety of people and situations."

**Sgt. Richards, CPD's commanding officer on the task force, added, "I like bringing fugitives to justice and locking up bad guys. On this squad I get to do that almost every day."**

On this particular day, however, there would be no arrest. The team moved into place in unmarked vehicles, setting up to cover the front and back of the house where the felon was living. But when the search warrant was executed, the only people in the residence were a woman and her young daughter. The search did turn up the shotgun, under the felon's mattress. He was now a fugitive and would eventually be arrested.

**Quinn noted that despite the different law enforcement organizations they belong to, there is a strong bond among VC1 members. "The task force setting breaks down barriers between agencies," he said. "Everyone works together as a team."**

That teamwork pays dividends beyond the task force, too. Relationships have expanded over time so that agents and detectives working all kinds of cases can pick up the phone and get help from their local and federal partners. "Agents and detectives all over the city have each other on speed dial," Sgt. Richards said.

And members of the task force are always ready to respond, Quinn said. "Whenever there is a murder, kidnapping, or multiple bank robberies and a call goes out for volunteers, even on weekends and evenings, we always get more people than we need." He added, "If someone is looking for a 9-to-5 type of job in law enforcement, VC1 is definitely not for them."

# The 'Whitey' Bulger Case

## New Campaign Focuses on Mobster's Companion

Investigators hope a new media campaign announced today will bring them closer to capturing the notorious mobster and Top Ten fugitive James "Whitey" Bulger by focusing public attention on his longtime companion Catherine Greig.

**Bulger, who once ran South Boston's violent Winter Hill Gang and is wanted for his role in 19 murders, has been pursued around the world by the FBI-led Bulger Fugitive Task Force for the past 16 years.**

"In terms of publicity, the FBI knows that combining the reach and power of the media with alert citizens is a successful formula for catching fugitives," said Richard Teahan, a special agent in our Boston office who leads the Bulger task force. "So we are taking the next logical step and continuing our focus on Greig, who has been on the run with Bulger since 1995."

The task force has produced a public service announcement (PSA) that will begin airing tomorrow on TV stations in 14 selected markets to make the public—and specifically women—aware of Greig's physical characteristics, habits, and personality traits.

"We are trying to reach a different audience that will produce new leads in the case," said Teahan, who has been tracking Bulger since 2006. "Greig has certain habits, characteristics, and idiosyncrasies that are recognizable, and we think the public might naturally notice these things. By running the PSA in markets where we believe Bulger has resided or may still have contacts," he added, "we increase our chances of getting a tip that will lead to Greig's whereabouts—and Bulger's capture."

**One of the things the public may notice, for example, is the more than 20-year age difference between Greig, 60, and Bulger, 81.** Some of Greig's other distinguishing characteristics include:

- She loves dogs and all kinds of animals.
- She is likely to have well-kept teeth because she previously worked as a dental hygienist.
- She likes to frequent beauty salons.
- Prior to her fleeing with Bulger, she had multiple plastic surgeries.

**Catherine Greig, as seen in 1982 (left), 1990 (top right), and in an artist's sketch.**

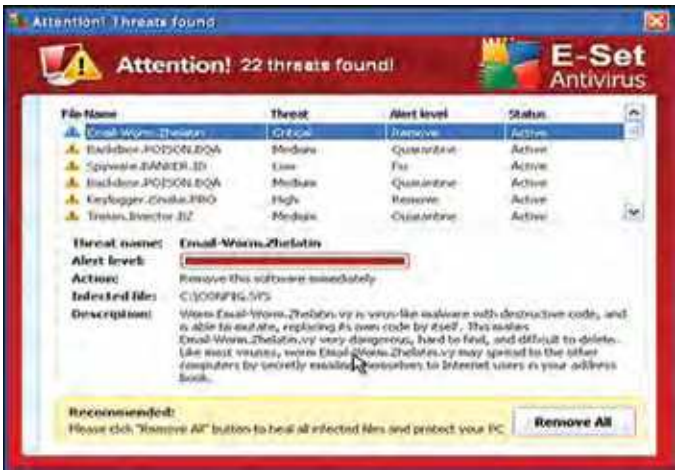
Greig has blue eyes, is 5 feet 6 inches tall, and had a thin build when she fled with Bulger. She is known to go by the aliases Helen Marshal and Carol Shapeton. She was last seen with Bulger in London in 2002. The 30-second PSA includes pictures of Greig after her pre-fugitive plastic surgeries.

Although she is not implicated in the crimes Bulger is wanted for, Greig was federally charged in 1997 for harboring a fugitive. There is a reward of up to $100,000 for her capture. **The reward for Bulger is up to $2 million, the largest the FBI has ever offered for a Top Ten domestic fugitive.**

"Whitey Bulger was the leader of a violent organized crime group in Boston," Teahan said. "He is charged with murder, extortion, racketeering, money laundering, and other crimes. We believe Greig fled with Bulger because she wanted to be with him, no matter what it took. It is important for the FBI to bring Bulger to justice," he added, "and Catherine Greig can lead us to him."

**We need your help.** If you have any information on Catherine Greig or Bulger's whereabouts, contact your local FBI office or the nearest U.S. Embassy or consulate.

*Editor's Note: James 'Whitey' Bulger and Catherine Greig were captured on June 22, 2011.* *See page 51 of this book for details.*




# 'Scareware' Distributors Targeted

## 12 Nations Coordinate Anti-Cyber Crime Effort

One of the most widespread types of cyber scam being perpetrated against consumers these days involves "scareware"—those pop-up messages you see on your computer saying you've got a virus and all you have to do to get rid of it is buy the antivirus software being advertised.

And if you don't buy it? The pop-ups continue unabated, and in some instances, the scareware renders all of the information on your computer inaccessible.

**But today, the Department of Justice and the FBI announced "Operation Trident Tribunal," a coordinated, international law enforcement action that disrupted the activities of two international cyber crime rings involved in the sale of scareware.** The groups are believed responsible for victimizing more than one million computer users and causing more than $74 million in total losses.

**Scam #1:** The FBI's Seattle office began looking into a scareware scam, later attributed to a group based in Kyiv, Ukraine, that ultimately claimed an estimated 960,000 victims who lost a total of $72 million. Investigators discovered a variety of ruses used to infect computers with scareware, including consumers being directed to webpages featuring fake computer scans that instead downloaded malicious software. The Security Service of Ukraine (SBU) deployed more than 100 officers as it orchestrated this phase of the operation in conjunction with the German BKA, Latvian State Police, and Cyprus National Police. Results included the execution of numerous search warrants, subject interviews, and seized bank accounts and a server.

**Scam #2:** The FBI's Minneapolis office initiated an investigation into an international criminal group using online advertising to spread its scareware product, a tactic known as "malvertising." According to a U.S. federal indictment unsealed today, two individuals in Latvia were charged with creating a phony advertising agency and claiming to represent a hotel chain that wanted to purchase online advertising space on a Minneapolis newspaper's website. After the ad was verified by the paper and posted, the defendants changed the ad's computer code so that visitors to the site became infected with a malicious software program that launched scareware on their computers. That scheme resulted in losses of about $2 million to its victims. The Latvian State Police led this phase of the operation, with the SBU and Cyprus National Police.

In a true reflection of the international nature of cyber crime, "Trident Tribunal" was the result of significant cooperation among 12 nations: Ukraine, Latvia, Germany, Netherlands, Cyprus, France, Lithuania, Romania, Canada, Sweden, the United Kingdom, and the U.S. So far, the case has resulted in two arrests abroad, along with the seizure of more than 40 computers, servers, and bank accounts. Because of the magnitude of the schemes, law enforcement agencies here and abroad are continuing their investigative efforts.

**How to spot scareware on your own computer:**

- Scareware pop-ups may look like actual warnings from your system, but upon closer inspection, some elements aren't fully functional. For instance, to appear authentic, you may see a list of reputable icons—like software companies or security publications—but you can't click through to go to those actual sites.
- Scareware pop-ups are hard to close, even after clicking on the "Close" or "X" button.
- Fake antivirus products are designed to appear legitimate, with names such as Virus Shield, Antivirus, or VirusRemover.

And to avoid being victimized, make sure your computer is using legitimate, up-to-date antivirus software, which can help detect and remove fraudulent scareware products.

# James 'Whitey' Bulger Captured

## Media Campaign Leads to Top Ten Arrest

Top Ten fugitive James "Whitey" Bulger was arrested thanks to a tip from the public—just days after a new media campaign was announced to help locate the gangster who had been on the run for 16 years.

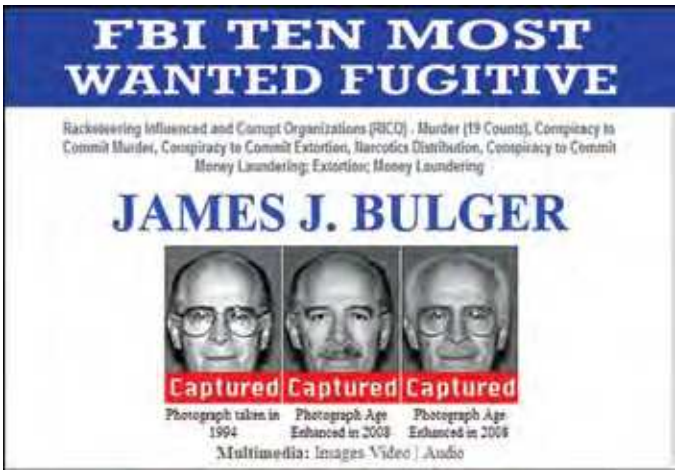
**Bulger, who once ran South Boston's violent Winter Hill Gang and was wanted for his role in 19 murders, was arrested with his longtime companion Catherine Greig Wednesday night in Santa Monica, California, by agents on our Violent Crimes Task Force.**

"Although there are those who doubted our resolve, it never wavered," said Boston Special Agent in Charge Richard DesLauriers. "We followed every lead, we explored every possibility, and when those leads ran out we did not sit back and wait for the phone to ring. The result is we have captured one of the FBI's Ten Most Wanted Fugitives, a man notorious in Boston and around the world for the very serious crimes he is alleged to have committed."

The FBI has always relied on cooperation from the public to help capture fugitives and solve crimes. The new media campaign regarding Bulger was designed to draw attention to Greig, who fled with Bulger in 1995. A 30-second public service announcement (PSA) produced by the Bureau began airing Tuesday in 10 states where it was believed Bulger had resided or still had contacts. California was one of those states.

The PSA focused on the 60-year-old Greig's physical appearance, habits, and personality traits and was directed specifically at women who might come in contact with her at places such as the beauty parlor or doctor's office. After the PSA began to air, hundreds of tips flowed into the FBI, and one of them led to the arrest Wednesday night in a residence near Los Angeles.

"We were trying to reach a different audience to produce new leads in the case," said Richard Teahan, a special agent in our Boston office who heads a task force that has searched for Bulger around the world. "We believed that locating Greig would lead us to Bulger. And that's exactly what happened."




The PSA included pictures of Greig after her pre-fugitive plastic surgeries and other details including her love of animals and the reward of up to $100,000 for her capture. Although she was not implicated in Bulger's crimes, Greig was federally charged in 1997 for harboring a fugitive. The reward for Bulger is up to $2 million—the largest the FBI has ever offered for a Top Ten domestic fugitive.

Bulger, 81, who is known for his violent temper, was arrested without incident and was scheduled to appear in a Los Angeles court later today.

# The Chicago Mafia

## Down but Not Out

A Roman Catholic priest and former prison chaplain who ministered to Chicago mob boss Frank Calabrese, Sr., was indicted earlier this month for illegally passing jailhouse messages from Calabrese and plotting with his associates on the outside—a sobering reminder of how deeply organized crime can reach into the community, even from behind bars.

**"Members of the mob will go to almost any lengths to carry out their criminal activity," said Special Agent Ted McNamara, a veteran investigator who supervises the La Cosa Nostra (LCN) organized crime squad in our Chicago Field Office.**

Calabrese, Sr., was sentenced to life in prison in 2009 for his role in 18 gangland slayings in the Chicago area dating back to 1970. His arrest—along with 13 others—was part of one of the most successful organized crime cases in FBI history, an eight-year investigation called Operation Family Secrets.

Because of the Family Secrets case—in which Calabrese's son testified against him—"the Chicago mob does not have the power and influence it once had," McNamara said. "But the mob still operates, and its members still represent a potentially serious criminal threat."

Unlike New York's infamous Five Families, the Chicago mob consists of only one family, often referred to as the "Outfit." It is organized under a variety of crews that engage in various criminal activities. A portion of the crews' illegal gains goes to the Outfit's top bosses.

"New York gets most of the attention regarding LCN," McNamara said, "but historically, going back to the days of Al Capone, Chicago LCN has always been a player, particularly in places like Las Vegas."

Unlike their New York counterparts, the Outfit has traditionally stayed away from drug trafficking, preferring instead crimes such as loan-sharking and online gambling operations and capitalizing on other profitable vices. One of the reasons it is so difficult to completely stamp out mob activity, McNamara said, is that over time the crews have insinuated themselves into unions and legitimate businesses.

**"Typically they get into running restaurants and other legal businesses that they can use to hide money gained from their illicit activities," McNamara explained.** "Over the years the Outfit has learned that killing people brings too much heat from law enforcement. Today they might not even beat up a businessman who doesn't pay back a debt," he added. Instead, they take a piece of his business, and then, over time, exercise more and more control over the company.

The Family Secrets case, which began in 1999 and resulted in the indictment of 14 subjects in 2005 for racketeering and murder, dealt a crushing blow to the Chicago mob. "Our goal now," McNamara said, "is to keep them from gaining strength again. We've got them down, and we've got to keep them down."

He noted that some of the mobsters currently in jail as a result of numerous prosecutions will be getting out in the next few years, and they will be under pressure to start making money again for the Outfit's top bosses.

"As long as there is money to be made from criminal activity," McNamara said, "these guys will never stop. So we need to continue to be vigilant and take the long view. The work we do on the LCN squad requires a lot of patience."

# Public Corruption Update

## A Busy Month Comes to a Close

The FBI works plenty of high-profile public corruption cases—including the investigation of former Illinois governor Rod Blagojevich, who was convicted Monday after previous indictments.

But many of our cases—worked closely with our investigative and prosecutive partners—don't make national news. Yet they are just as vital to our public corruption mandate—to root out those who violate the public trust. In fact, June was a particularly busy month on that front. From Florida to Arizona, there were a string of legal actions taken against public officials serving in a variety of positions.

**Here are some examples:**

- Two commissioners in Lackawanna County, Pennsylvania were convicted of racketeering and other charges in connection with accepting and demanding payments and other benefits from people doing business with the county.
- A Nashville, Tennessee police officer was indicted for accepting cash while delivering drugs and drug money to several locations for local drug dealers—all while wearing his uniform and driving his police car.
- A special agent with the U.S. Immigration and Customs Enforcement's Homeland Security Investigations was arrested in Arizona on charges that she illegally accessed, stole, and transferred sensitive government documents to family members and associates with strong ties to drug trafficking organizations.
- A county judge in Cleveland was convicted of accepting bribes, including campaign contributions, in return for fixing cases. So far, this particular investigation has implicated dozens of elected officials, public employees, and contractors within the county.
- A former mayor and a magistrate from South Daytona, Florida were both charged with accepting bribes from purported investors in exchange for lowering city code liens on a large investment property.

**Currently, the FBI—with our partners—is working more than 2,000 corruption investigations involving public officials around the country.** These investigative efforts certainly pay off—during fiscal year 2010, our cases led to more 1,330 informations/indictments and over 900 convictions (primarily at the federal level but also some at the local level).

Our ability to use sophisticated investigative tools and methods—like undercover operations—is one of the reasons why the FBI is in a unique position to investigate allegations of corruption. These tools and methods often give investigators a front-row seat to witness the actual exchange of bribe money or a handshake that seals an illegal deal.

Bribery is the most common form of corruption the Bureau investigates. But there are plenty more crimes—including extortion, embezzlement, racketeering, kickbacks, money laundering, and all sorts of fraud. A significant portion of our cases involve border corruption.

**At the end of the day, the majority of public officials are honest, hard-working individuals determined to improve the lives of their fellow citizens.** But a small number of elected, appointed, or contracted officials are only focused on their own good. The actions of corrupt officials—often with the help of private sector accomplices—undermine democratic institutions and threaten national security, which is why the FBI ranks public corruption as our top criminal priority.


Left: Charges against the subjects included smuggling real and phony drugs and other contraband into the U.S., along with counterfeit $100 bills.

# Operation Smoking Dragon

## Part 1: Dismantling an International Smuggling Ring

The judge who recently sentenced Yi Qing Chen noted that the smuggler "never saw a criminal scheme he didn't want a part of." The Southern California man was convicted last October of distributing methamphetamine, trafficking approximately 800,000 cases of counterfeit cigarettes, and conspiring to import Chinese-made shoulder-fired missiles into the U.S.

**Chen is now serving a 25-year prison sentence, and his case marks the end of a long-running investigation called Operation Smoking Dragon.**

Smoking Dragon and a related case in New Jersey called Operation Royal Charm led to the indictment of 87 individuals from China, Taiwan, Canada, and the U.S. The investigations uncovered—and dismantled—an international smuggling ring that could have threatened the country's national security.

Charges against the subjects included smuggling real and phony drugs and other contraband into the U.S. along with counterfeit $100 bills—believed to have been produced in North Korea—that were so nearly perfect and so much more sophisticated than typical counterfeit currency they were dubbed "Supernotes."

"One of the most important things about Operation Smoking Dragon was that it demonstrated the broad range of international criminal activity conducted by today's Asian organized crime groups," said Special Agent Bud Spencer, who worked the case in our Los Angeles office.

**The eight-year investigation began when FBI undercover agents, posing as underworld criminals, helped make sure that shipping containers full of counterfeit cigarettes made it past U.S. Customs officers undetected.** Over time, as undercover agents won the smugglers' trust, they were asked to facilitate other illegal shipments such as narcotics and millions of dollars in Supernotes. Later, the smugglers offered a variety of Chinese military-grade weapons, including the QW-2 surface-to-air missiles.

Some of the drugs—including methamphetamine and fake Viagra—were hidden in large cardboard boxes with false bottoms that contained toys. The Supernotes were placed between the pages of books or lined in large bolts of rolled-up fabric. All of the items were smuggled into the U.S. in 40-foot shipping containers.

Between Smoking Dragon and Royal Charm, some $4.5 million in counterfeit currency was seized, along with more than $40 million worth of counterfeit cigarettes, drugs, and other real and phony items. The smugglers were also forced to forfeit a total of $24 million in cash, along with real estate, cars, and jewelry.

Most of the defendants were indicted in 2005 and have since pled guilty or been convicted. Chen was the final defendant to be sentenced relating to Operation Smoking Dragon. His was the nation's first conviction under a 2004 anti-terrorism statute that outlaws the importation of missile systems designed to destroy aircraft.

"There is only one purpose for shoulder-fired missiles like the QW-2, and that is to bring down aircraft," said Special Agent Omar Trevino, who worked the case from the beginning. "Smoking Dragon dismantled an international smuggling ring, and it illustrated that organized crime groups will stop at nothing to make a profit."

Mark Aveis, an assistant United States attorney in Los Angeles who prosecuted the Chen case, agreed with Agent Trevino. "Chen and his associates didn't care what they smuggled as long as they made money," he said. "This case highlights the FBI's ability to carry out successful long-term undercover investigations—and the continuing need for such investigations."

# Iraqi Antiquities Returned

## Artifacts Seized During Public Corruption Investigation

Terracotta plaques and other artifacts seized during a 2006 investigation were returned to the government of Iraq today in a Washington, D.C. ceremony that celebrated a successful law enforcement operation and the cultural significance of antiquities that are thousands of years old.

**"These artifacts are truly invaluable," said Ron Hosko, special agent in charge of the Criminal Division in our Washington Field Office. "The FBI is pleased to be able to return them to their rightful owner."**

The artifacts—some small enough to be held in the palm of one's hand—were seized during a public corruption investigation conducted by our International Contract Corruption Task Force, a multi-agency task force whose mission is to stop fraud and corruption related to U.S. reconstruction efforts in Iraq, Afghanistan, and elsewhere overseas.

The artifacts were illegally taken in 2004 by Department of Defense contractors who were traveling through the Babylon region of Iraq. Investigators learned that the contractors collected the items and used them as gifts and bribes or sold them to other contractors who then smuggled them into the United States. Two of the contractors were sentenced to prison for their roles in the fraud scheme.

"The FBI is committed to identifying and preventing corruption and contract fraud no matter where it takes place," Hosko said during the ceremony at the Iraqi Cultural Center. "Working abroad does not entitle anyone to remove historic artifacts and treat them as mementos for illegal sale."

Iraqi Ambassador to the United States Shakir Mahmood Sumaida'ie expressed his gratitude to the FBI and U.S. Immigration and Customs Enforcement, which also returned items from a separate case. As Iraq works to "reconstruct our country and our heritage," the ambassador said, "We are grateful for the cooperation from the American authorities."

**Agents on the FBI's art crime team—who receive specialized training in art and cultural property investigations—were called in recently to help authenticate the artifacts and to facilitate their return to Iraq.**

**The seized artifacts include these vases and range in age from 2,500 to 4,000 years old.**

The items include two pottery dishes, four vases, an oil lamp, three small statues, and the seven terracotta relief plaques. They range in age from 2,500 to 4,000 years old—from the Old Babylonian period to the Neo-Assyrian or Neo-Babylon periods.

The terracotta plaques were made with clay and pressed into a mold that was then fired in an oven. Although it is not clear exactly how the plaques were used, experts believe they were thought to provide magical protection against evil or sickness. The plaques depict a warrior goddess, a woman with child, and two boxers, among other scenes, and could have been carried for personal devotion or displayed in temples or buried in foundations of buildings.

It was the looting of the Baghdad Museum in Iraq in 2003 that led to the formation of the FBI's art crime team the following year. "We realized then that we needed a group of agents who were specially trained in the area of stolen and looted art," said Bonnie Magness-Gardiner, who manages our art theft program. Since its inception, the art crime team has recovered more than 2,600 items valued at over $142 million.

Hosko added that the recovery of the antiquities during a case focused primarily on public corruption illustrates how the FBI's intelligence-driven approach to investigations often leads to uncovering additional criminal activity.

Left: San Diego FBI Special Agent in Charge Keith Slotter, with correspondent Lynn Stuart, is interviewed for *San Diego's Most Wanted*, a 30-minute program that airs Saturday nights.

# 'San Diego's Most Wanted'

## Show Celebrates First Anniversary, 57 Captures

The lights were on and the cameras were rolling as the special agent in charge of our San Diego office got his cue: "This is *San Diego's Most Wanted*. I'm Keith Slotter. Thanks for inviting us into your home. Tonight, a rash of robbers, pill-pinching thieves, and a criminal carjacker. We need your help to find them."

**So began the taping of another episode of the FBI's 30-minute weekly television show that runs Saturday nights in prime time on San Diego's Fox affiliate, KSWB.**

The show, based on the *America's Most Wanted* format, celebrated its one-year anniversary recently with an impressive statistic: 57 criminals have been apprehended as a result of good police work and viewer tips.

"The main mission of the show is to catch bad guys," said Slotter, who hosts *San Diego's Most Wanted* along with correspondent Lynn Stuart. Viewer tips have led to the arrest of bank robbers, parole violators, and murderers. The very first capture was a man wanted since 2007 on child molestation charges.

Each week's cases—drawn from FBI investigations and local police departments—feature fugitives, thieves, and violent criminals who have active warrants for their arrest. Missing children are also publicized, which explains the recent on-location filming at the National Center for Missing & Exploited Children in Washington, D.C.

"The show offers a tremendous opportunity to reach the public about San Diego's most wanted criminals," Slotter said during a break in filming. "And it's also an incredible opportunity to partner with local law enforcement and to build relationships in the community. Where else are we going to get 30 minutes each week to talk about cases and initiatives involving all of San Diego's law enforcement agencies?"

"The show really is a great crime-fighting tool," said Lt. Andra Brown, San Diego Police Department's public information officer. The department has captured a number of criminals as a result of the show, she noted. "We are very happy with our FBI partnership."

Lt. Brown added that the program's informational segments are also helpful. Recent and upcoming tips on how not to be a robbery victim and scams targeting the elderly, for example, provide valuable public safety information.

***San Diego's Most Wanted* airs Saturday nights at 7:30 p.m. and is repeated Sunday nights at 11 p.m. Tips are received from all over San Diego County as well as from across the border in Tijuana, Mexico.** Agents are on hand to take viewers' information and pass it on to the appropriate law enforcement agency. Tipsters—who can remain anonymous—are eligible for rewards of up to $1,000 for information leading to the capture of those featured on the show.

The idea for *San Diego's Most Wanted* was an outgrowth of Slotter's regular monthly appearances on Fox 5's morning news program, where he talked about public safety matters, crime issues, and high-priority FBI cases in the San Diego area. "He understands the importance of working with the public and the media to help solve crimes," said Special Agent Darrell Foxworth, who helps produce the show. And having San Diego's top FBI agent as the host, he added, gives the program "instant credibility."

As the episode taping drew to a close recently, Slotter told viewers, "Your tips could be all it takes to get these criminals off our streets." He added, "We're sure not going to rest until these fugitives are tracked down and caught. I promise you that."

# Taking a Trip to the ATM?

## Beware of 'Skimmers'

Last fall, two brothers from Bulgaria were charged in U.S. federal court in New York with using stolen bank account information to defraud two banks of more than $1 million.

Their scheme involved installing surreptitious surveillance equipment on New York City ATMs that allowed them to record customers' account information and PINs, create their own bank cards, and steal from customer accounts.

What these two did is called "ATM skimming"—basically placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine. ATM skimming is a growing criminal activity that some experts believe costs U.S. banks hundreds of millions of dollars annually.

The devices planted on ATMs are usually undetectable by users—the makers of this equipment have become very adept at creating them, often from plastic or plaster, so that they blend right into the ATM's façade. The specific device used is often a realistic-looking card reader placed over the factory-installed card reader. Customers insert their ATM card into the phony reader, and their account info is swiped and stored on a small attached laptop or cell phone or sent wirelessly to the criminals waiting nearby.

In addition, skimming typically involves the use of a hidden camera, installed on or near an ATM, to record customers' entry of their PINs into the ATM's keypad. We have also seen instances where, instead of a hidden camera, criminals attach a phony keypad on top of the real keypad...which records every keystroke as customers punch in their PINs.

Skimming devices are installed for short periods of time—usually just a few hours—so they're often attached to an ATM by nothing more than double-sided tape. They are then removed by the criminals, who download the stolen account information and encode it onto blank cards. The cards are used to make withdrawals from victims' accounts at other ATMs.

Because of its financial jurisdiction, a large number of ATM skimming cases are investigated by the U.S. Secret Service. But through FBI investigative experience, we have learned that ATM skimming is a favorite activity of Eurasian crime groups, so we sometimes investigate skimming—often partnering with the Secret Service—as part of larger organized crime cases.

**Skimming typically involves the use of hidden cameras (top) to record customers' PINs and phony keypads (right) placed over real keypads to record keystrokes.**

Some recent case examples:

- In Miami, four Romanians were charged with fraud and identity theft after they made and placed skimming devices on ATMs throughout four Florida counties…all four men eventually pled guilty.
- In Atlanta, two Romanians were charged and pled guilty to being part of a criminal crew that stole account information from nearly 400 bank customers through the use of skimming equipment they installed on ATMs in the Atlanta metro area.
- In Chicago, a Serbian national was arrested—and eventually pled guilty—for attempting to purchase an ATM skimming device, hoping to steal information from ATM users and loot their bank accounts.
- In New York, a Bulgarian national referenced at the top of this story was sentenced yesterday to 21 months in prison for his role in a scheme that used sophisticated skimming devices on ATMs to steal over $1.8 million from at least 1,400 customer accounts at New York City area banks.

One last note: ATMs aren't the only target of skimmers—we've also seen it at gas pumps and other point-of-sale locations where customers swipe their cards and enter their PIN.

Left: The international smuggling ring brought illegal drugs, cigarettes, and counterfeit currency into the country.

# Operation Smoking Dragon

## Part 2: An Undercover Agent Tells His Story

Operation Smoking Dragon and a related case led to the indictment of 87 individuals and dismantled an international smuggling ring that brought illegal drugs, cigarettes, and counterfeit currency into the country—and conspired to bring in Chinese-made weapons as well.

Retired Special Agent Bob Hamer worked undercover on Operation Smoking Dragon and was instrumental in the investigation's success. During his 26-year career with the Bureau, Hamer specialized in covert work, posing as a drug dealer, screenwriter, friend of the Mafia, even a pedophile. Below, he talks about Operation Smoking Dragon and his work undercover.

**Q: How did you get involved with Smoking Dragon?**

**Mr. Hamer:** The case agent was looking for an undercover agent to help target an Asian organized crime group, and he contacted me. I met with the agent and his informant. The informant liked me and set up a meeting with the person we believed was the largest importer of counterfeit cigarettes on the West Coast. And that was it. I was in.

**Q: How did you convince the target that you could be trusted?**

**Mr. Hamer:** My story was that I had inherited my grandfather's trust and that I was a savvy investor. More importantly, I had a warehouse where they could store the cigarettes, and I had access to long-haul truck drivers and some contacts at the port that might be able to help them get their shipping containers into the country. The bad guys bought it.

**Q: How was Smoking Dragon different from other undercover cases you worked?**

**Mr. Hamer:** Most of my undercover assignments were pretty straightforward investigations, from point A to point B. Smoking Dragon was one of those cases that started at A and went all over the alphabet. We assumed it was just going to be about cigarettes. We never thought it would expand to surface-to-air missiles or counterfeit currency—the Supernotes. We didn't think drugs would be involved or other counterfeit goods.

**Q: You started on the case in 2002 and worked it until indictments were handed down in 2005. Was this the longest undercover assignment you had?**

**Mr. Hamer:** Yes. I was undercover on Smoking Dragon for almost three years. As the case progressed beyond the initial target, I was dealing with one target or another almost on a daily basis. I think we added it up once that I had over 1,000 separate conversations during those three years with all the various targets. It was a full-time assignment, although I was working two other undercover operations at the same time.

Drugs such as methamphetamine and Ecstasy were among the items smuggled into the country by boat in 40-foot shipping containers.

**Q: Why was this case so important?**

**Mr. Hamer:** I considered one of the targets to be the most dangerous man in America. Whatever we wanted, whatever we brought up, he was capable of getting. He brought us the weapons deal, the Supernotes deal. He was

doing cigarettes, Ecstasy. He was talking about setting up a crystal meth lab. This guy could put you together with anybody to make any deal. He said he could get us any weapons—anything but nuclear weapons—and I think he could have. Whatever China had, this guy was capable of getting. To me he was dangerous, not in the sense that he could kill you with his bare hands, but because of his connections. He was a broker for everything.


More than $40 million worth of counterfeit cigarettes, like the cartons of Marlboros shown above, were seized.

**Q: How did you get started doing undercover work?**

**Mr. Hamer:** I reported to my first FBI office in San Diego in September 1979, and within six months I assumed my first undercover role. I always thought it would be exciting to be part of an undercover investigation. We were doing an organized crime case, and I volunteered to go undercover. An informant introduced me to his colleague who would become our target. That very first meeting my knees were shaking so much—not from fear but from adrenaline—I prayed nobody would notice. I met the target, and we hit it off. I came away with an adrenaline high that lasted for the rest of my career. I loved the work and did 20 separate undercover assignments in all, some of which lasted a day or two and some that ran for years.

**Q: What does it take to be good at undercover work?**

**Mr. Hamer:** You have to build a story that you believe and that you can sell. You have to love the work and believe in yourself. You've got to be quick on your feet, but you can't dominate the conversation. You have to know who you are both in the real world and the undercover world, because you are on a high wire without a net. In Hollywood you get a chance to say your lines again if you make a mistake. There are no retakes in the real world. If you make a mistake on the street, you might blow the case or risk getting yourself killed.

**Q: Do you develop an emotional connection to the people you are investigating?**

**Mr. Hamer:** That's an issue, but it comes back to knowing who the real you is. You have to be one of the bad guys without becoming one of them. There is a line you can't cross. You have to walk up to that line, but you can't go over it.

**Q: You retired at age 56, one year after the Smoking Dragon indictments were announced and one year before agents are required to retire. Do you miss the undercover life?**

**Mr. Hamer:** Smoking Dragon was one of the biggest cases I worked. With only one year to go before mandatory retirement, I didn't think I could top Smoking Dragon, so I retired. I do miss the work. I miss the adrenaline rush of being undercover, but not to the point that I would go work for some private detective agency. If the FBI called me back, yeah, I would love it. I had 26 great years in the FBI.


Levi's jeans manufactured in China and smuggled into the U.S. looked real enough, but they were fakes.


# Foreclosure Fraud

## Victims Lose Their Shirts… and Their Homes

He was their last hope—about 250 Southern California homeowners facing foreclosure and eviction believed him when he said he could save their homes.

But in reality, he was their worst nightmare—he ended up fleecing the homeowners for approximately $1 million…and not a single home was saved in the process.

Last week, Jeff McGrue, owner of a Los Angeles-area foreclosure relief business, was sentenced to 25 years in prison for defrauding people who were at the end of their rope. Even the federal judge who sentenced him called him "heartless."

**It all started in late 2007,** when McGrue—and several other conspirators who have pled guilty—orchestrated the scheme primarily through his company Gateway International. He paid unwitting real estate agents and others to serve as "consultants" to recruit customers who were facing foreclosure or were "upside-down" on their mortgages—meaning they owed more than their homes were worth. Many of the customers didn't understand English or the contracts they were signing.

**How the scam worked.** McGrue and associates told the homeowners that "bonded promissory notes" drawn on a U.S. Treasury Department account would be sent to lenders to pay off mortgage loans and stop foreclosure proceedings; that lenders were required by law to accept the notes; and that homeowners could buy their homes back from Gateway and receive $25,000, regardless of whether they decided to re-purchase.

The payback for McGrue? The homeowners had to fork over an upfront fee ranging from $1,500 to $2,000…sign over the titles of their homes to Gateway…and pay Gateway half of their previous mortgage amount as rent for as long as they lived in the house.

**Of course, nothing that McGrue told his victims was true:** he didn't own any bonds or have a U.S. Treasury account, plus the Treasury doesn't even maintain accounts that can be used to make third-party payments. Lenders weren't legally obligated to accept bonded promissory notes, which were worthless anyway. And Gateway International had no intention of selling back the properties to the homeowners. Evidence shown at McGrue's trial revealed that it was his intent to re-sell the homes, once they were titled in Gateway's name, to unsuspecting buyers.

The FBI began its investigation in 2008, after receiving a complaint from one of the victims.

**During these uncertain economic times, there are many unscrupulous people looking to line their pockets at the expense of others' misfortunes.** One of the most effective ways to defend yourself against foreclosure fraud is awareness. According to the Federal Trade Commission, if you or someone you know is looking for a loan modification or other help to save a home, avoid any business that:

- Offers a guarantee to get you a loan modification or stop the foreclosure process;
- Tells you not to contact your lender, lawyer, or a housing counselor;
- Requests upfront fees before providing you with any services;
- Encourages you to transfer your property deed to title to them;
- Accepts payment only by cashier's check or wire transfer; or
- Pressures you to sign papers you haven't had the chance to read thoroughly or that you don't understand.

Contact your local authorities or your state's attorney general if you think you've been a victim of foreclosure fraud.

# WMD Central

## Part 1: Five Years and Building

*Five years ago this week, the FBI established its first Weapons of Mass Destruction (WMD) Directorate to centralize and coordinate all WMD-related investigative activities, intelligence analysis capabilities, and technical expertise from across the Bureau. Recently, FBI.gov spoke with Dr. Vahid Majidi—the head of the WMD Directorate since its launch—on his office's work over the past five years. Today, he talks about the current threat and specific focus of the directorate. Later this week, he'll discuss case examples, lessons learned, and the future of the directorate.*

**Q. Why was the directorate created?**

**Dr. Majidi:** The FBI has been in the WMD business for quite some time, more formally since 1995 when we created a program in our Counterterrorism Division to address the WMD threat. But obviously, a lot has happened in recent years. And it became clear that our WMD response crossed operational lines and also involved our counterintelligence, criminal, and cyber programs—not to mention the response and forensics expertise in the FBI Laboratory and the render-safe capabilities of our Critical Incident Response Group. We needed a single force to coordinate all of our WMD activities. The directorate gives us that.

**Q. What does the WMD threat look like today?**

**Dr. Majidi:** The nature of the threat hasn't changed all that much over the past decade. International terrorist groups are still determined to get their hands on various forms of weapons of mass destruction—chemical, biological, radiological, and nuclear. Organizations and nation states still want material and expertise for their own programs. And certain domestic groups are still trying to acquire materials needed for basic WMD applications—predominately chemical or biological in nature.

Dr. Vahid Majidi

**Q. What about all those white powder letters?**

**Dr. Majidi:** Most turn out to be hoaxes, and they require a lot of investigative resources, but we have to investigate each and every incident. You never know when one of them will be real.

Members of the FBI's Hazardous Materials Response Unit enter a home suspected of biological contamination. AP photo.

**Q. Can you briefly explain how the WMD Directorate works?**

**Dr. Majidi:** Absolutely. The main focus of our WMD Directorate—and the primary focus of our overall efforts—is prevention, to keep a WMD attack from ever taking place. To make that happen, we have several closely integrated activities that pull together resources from various parts of the FBI. Our countermeasures and preventions group includes a full spectrum of activities, from WMD training for domestic and international law enforcement partners…to outreach efforts to academia, industry, government, and retailers to help them spot indicators of potential WMD activity…to working with our government partners to formulate sound policies. The investigations and operations group addresses threatened or actual use of weapons of mass destruction, or the transfer of materials, knowledge, and technology needed to create a WMD. We also can and do collect evidence in contaminated areas, disarm hazardous devices, and provide command and control support in on-scene activities. Finally, our intelligence and analysis group serves as the foundation of our proactive approach to threats. Our analysts sort through data to identify relevant WMD information, and our agents work to identify sources of valuable intelligence. And because we are part of the intelligence community, we share information routinely with our partners. Through it all, we have a lot of activities and capabilities in play, and I think we're making a real difference.

Left: Dr. Vahid Majidi

# WMD Central

## Part 2: Looking Back, Looking Ahead

*Our interview continues with Dr. Vahid Majidi, head of our Weapons of Mass Destruction, or WMD, Directorate, which marked its fifth anniversary on July 26.*

**Q. Can you provide a few examples of successful WMD investigations over the past five years?**

**Dr. Majidi:** We've managed quite a few cases actually, including our first major counterproliferation investigation that involved two Iranian men and one Iranian-American who were charged in California with conspiring to export certain technologies from the U.S. to Iran. Other examples include a Texas man charged with possessing 62 pounds of sodium cyanide; a government contractor in Tennessee charged with trying to sell restricted U.S. Department of Energy materials; and a Nevada man charged with possessing deadly ricin.

**Q. What has the FBI learned over the past five years?**

**Dr. Majidi:** Quite a bit. For some time, we've had WMD coordinators in every one of our field offices. But we realize that for WMD prevention to be truly comprehensive, we need to think and act globally. So that's why—in addition to our network of legal attaché offices and agents around the world—we've recently put our first WMD coordinators overseas, in our offices in Tbilsi and Singapore. We also have personnel assigned to Interpol to help it develop an international WMD training program like ours.

**Q. What kind of work is done overseas?**

**Dr. Majidi:** It runs the gamut. For instance, several years ago, after an interdiction of highly enriched uranium in Georgia in the former Soviet Union, our WMD experts performed a forensic analysis of the material and then testified in Georgian courts. And when the Russian defector in London was poisoned with a radioactive isotope in 2006, our WMD personnel shadowed London Metropolitan Police during the ensuing investigation to develop lessons learned to help us prepare for such a scenario here. Through it all, we've built some strong relationships with our global partners.

**Q. What are the WMD Directorate's plans for the next five years?**

**Dr. Majidi:** The basic knowledge and material that go into making weapons of mass destruction is becoming more readily available to anyone, anywhere in the world as the Information Age matures. That's why we'll continue to be all about partnerships—locally, nationally, and internationally. We'll also focus even more on threats on the horizon. For example, we'll look at emerging developments like synthetic biology from a preventative point of view. By collaborating with the synthetic biology community, we can articulate our safety and security concerns as they relate to weapons of mass destruction. We'll also be improving our threat analysis capabilities to better spot potential WMD opportunities, potential WMD vulnerabilities, and gaps in our intelligence collection.

**Q. What can the average citizen do to assist law enforcement with the WMD threat?**

**Dr. Majidi:** Keep in mind that to develop weapons of mass destruction, you only need two things: the material and the know-how. So please, if you see anything suspicious or in a place where it doesn't belong, report it to local law enforcement or your closest FBI Joint Terrorism Task Force. It could be just the tip we need to stop something serious.

# A Byte Out of History

## Going SOLO: Communist Agent Tells All

In April 1958, a representative of the Communist Party of the United States (CPUSA) named Morris Childs made important trips to the Soviet Union and China. His purpose: to re-establish formal contact between the CPUSA and these countries.

First, Morris visited with key Communist Party and Soviet leaders in Moscow. He learned of their wider political goals, their concerns and fears, and their deep interest in restoring connections with the CPUSA. Then he went to Beijing, where he made similar inroads and met with Premier Mao Tse Tung.

After three months, Morris returned home and reported all he'd learned to CPUSA leaders. But as a new Freedom of Information Act release in the FBI Vault makes clear, he was also secretly talking to President Dwight Eisenhower, the vice president, the secretary of state, and a select group of other U.S. officials.

**Morris, you see, was actually one of the FBI's greatest Cold War agents.**

Born Moishe Chilovsky in the Ukraine, Morris Childs and his family immigrated to the U.S. in 1912. He joined the emerging communist movement in Chicago as a teenager and devoted his life to the cause. In 1947, his work ended after an internal power struggle removed him as editor of the CPUSA's flagship newspaper and his continuing struggle with heart disease left him sickly and incapacitated. Unable to pursue other work for the movement, Childs was soon forgotten.

**Meanwhile, America's growing realization of the penetration of the U.S. government by the Soviets and the subsequent political debate over the role of communism in society became the focus of the day.** By the early 1950s, the FBI began taking a more proactive approach to dealing with Soviet intelligence. That included zeroing in on the CPUSA—in part, by approaching Communist officials who had left the party. One of the first on the list was Morris Childs' brother Jack.

Jack willingly cooperated and strongly advocated that the Bureau contact his brother, paving the way for a 1952 meeting between Morris and Special Agent Carl Freyman. The two got along quite well, sharing a knowledge of communist philosophy and an interest in wider intellectual and cultural issues.

**Morris Childs' intelligence work was handled by the FBI under the code name SOLO.**

After several meetings, Childs agreed to return to the CPUSA as an informant for the FBI. With the assistance of Jack, the Bureau helped Morris rehabilitate both his health and his role in the Party. Morris began feeling better after a Bureau-arranged stay at the Mayo Clinic, and within a year he started reaching out to his old comrades. He and Jack were accepted back into the CPUSA and eventually were tasked with deepening contacts with the Canadian Communist Party and through it, the Soviet Union.

Over four decades, Morris made more than 50 visits overseas for the CPUSA, each time reporting with great detail and insight about the issues and concerns of the leadership of the Soviet Union and China. Considering that these two nations were such closed societies, Morris's intelligence was invaluable—a fact recognized by President Ronald Reagan when he awarded Morris (and posthumously, Jack) with the Presidential Medal of Freedom.

The intelligence work of the brothers—and later their wives—was handled by the FBI under the code name SOLO. In the coming months, stay tuned as we reveal more details of this long-running operation as additional sections of the SOLO file are released in our Vault.


# The FBI's Child ID App

## Putting Safety in Your Hands

You're shopping at the mall with your children when one of them suddenly disappears. A quick search of the nearby area is unsuccessful. What do you do?

**Now there's a free new tool from the FBI that can help.** Our just launched Child ID app—the first mobile application created by the FBI—provides a convenient place to electronically store photos and vital information about your children so that it's literally right at hand if you need it. You can show the pictures and provide physical identifiers such as height and weight to security or police officers on the spot. Using a special tab on the app, you can also quickly and easily e-mail the information to authorities with a few clicks.

The app also includes tips on keeping children safe as well as specific guidance on what to do in those first few crucial hours after a child goes missing.

**We encourage you to share the word about this app with family and friends, especially during upcoming activities in your communities to raise awareness on crime and drug prevention.** For its part, the FBI is working to publicize the app with the American Football Coaches Association (AFCA)—its long-time partner in the National Child Identification Program, which provides a physical kit to gather your child's pictures, fingerprints, personal characteristics, and even DNA to keep with you in case of emergency. The AFCA is producing a public service announcement about the app and will spread the word at various football games during the upcoming season.

Right now, the Child ID app is only available for use on iPhones and can only be downloaded for free from the App Store on iTunes, but we plan to expand this tool to other types of mobile devices in the near future. And we'll be adding new features—including the ability to upload other photos stored on your smart phone—in the coming weeks and months.

**An important note:** the FBI (and iTunes for that matter) is not collecting or storing any photos or information that you enter in the app. All data resides solely on your mobile device unless you need to send it to authorities. Please read your mobile provider's terms of service for information about the security of applications stored on your device.

Put your child's safety in your own hands. Download the FBI's Child ID app today.


*Editor's Note: In response to user feedback, the FBI Child ID app was updated with new features, including password protection and additional photo capabilities, in October 2011.*

# Civil Rights Program Update

## We Take Our Role Very Seriously

Last month, a Tennessee man received a life sentence for the racially motivated killing 10 years earlier of a county code enforcement officer who had simply been doing his job.

**The investigation of this murder was one of hundreds of civil rights cases the FBI opens each year.** It's a responsibility that—according to Eric Thomas, chief of our Civil Rights Unit at FBI Headquarters—"we take very seriously."

During fiscal year 2010, said Thomas, we initiated more than 750 civil rights cases that fell into one of four categories—hate crimes, color of law violations, human trafficking, and Freedom of Access to Clinic Entrances (FACE) Act violations.

**Thomas discussed each category in more detail:**

"…**Hate crimes,** almost a quarter of our 2010 civil rights caseload, are motivated by a particular bias against the victim—like skin color, religion, ethnicity, or country of origin—and includes such things as threats, cross burnings, assaults, and murder. In 2009, the Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act added sexual orientation, gender, gender identity, and disabilities to the list of biases. That law also allows us to prosecute violent hate crimes federally. Before that law, many violent hate crimes were prosecuted at the state level as traditional assaults, murders, etc.…"

"…**Color of law violations,** more than half of our civil rights investigations last year, involve actions taken by someone acting under the authority of the law—local, state, or federal. Most of these cases are initiated based on allegations of excessive force by law enforcement or correctional officers. However, there are others that involve allegations of sexual assault, theft, or deprivation of property…"

"…**Human trafficking,** just over 20 percent of our 2010 civil rights caseload, is a form of human slavery that cannot be tolerated. It's a growing problem that includes forced physical labor, forced household service, and sex trafficking involving international victims or adult U.S. citizens. (Note: Sex trafficking of U.S. children is handled by the FBI's Crimes Against Children program.) In early 2013, the FBI's uniform crime reporting program will

begin collecting data from our law enforcement partners on human trafficking offenses… "

"…**FACE Act violations** account for a smaller percentage of our workload—just over 2 percent last year. These crimes—committed against those who seek to obtain or provide reproductive health care services—include threatening phone calls and mail, property damage, blockades, assaults, and murders. In recent years, we've also seen a rise in bio-terrorism threats, especially hoax anthrax letters…"

**Intelligence** plays an important role in our civil rights program. "For example," explained Thomas, "we've established risk indicators for each of our subprogram areas to help field office agents and analysts better identify, assess, and ultimately address the civil rights threats within their regions."

**Collaboration** plays a vital role as well, said Thomas. "Many of our civil rights investigations—in particular, hate crimes and human trafficking—are enhanced by joint efforts with law enforcement partners. Many field offices participate in task forces and/or working groups focused on major civil rights threats." He also said the Bureau works closely with community and civic organizations at the local and national levels.

If you believe you've been the victim of or a witness to a civil rights crime, contact your local police department or FBI office.

# Fraud in the Family

## The Case of the Cheating Foster Parents

It's almost unthinkable—parents stealing from their own foster child. But here's a story about a couple who did exactly that.

It's also a case that Tampa FBI Agent Dan Kelly, Florida Department of Law Enforcement Agent Terry Corn, and Acting U.S. Attorney Robert O'Neill (now U.S. Attorney) won't soon forget. Said Kelly, "For financial crime investigations, we often don't get to know the victims, but in this instance, it was hard not to be absorbed into this boy's situation."

**It started back in 2000**, when 13-year-old Markus Kim suffered an unimaginable loss—his father murdered his mother. Markus was eventually placed with foster parents Radhames and Asia Oropeza in Flushing, New York.

About six months later, Markus learned he was entitled to a $500,000 life insurance policy that his mother had taken out. He couldn't access the money until he turned 18…in the interim it would be managed by the life insurance company. Not long after, Radhames and Asia Oropeza began suggesting that Markus consider real estate investing when he became of age.

Around the time Markus turned 18, his foster parents left New York without a word to him. Turns out they had moved to Florida, and about a year later, he was invited down to visit them. The Oropezas convinced their foster son to buy two $200,000 certificates of deposit (CDs) from a local bank…to better protect his money, they said. Because Markus trusted them, he followed their advice, and even allowed Asia Oropeza to co-sign bank documents.

The bank told Markus he'd receive monthly $1,000 checks—interest earned by the CDs. But after two checks, they stopped coming. He discovered that the CD accounts had been emptied and closed by Asia Oropeza.

**So how did the FBI become involved?** Markus, becoming exceedingly frustrated, contacted a legal aid attorney in New York, who in turn sought the help of an attorney in Florida. The attorney, who worked the case pro bono, contacted Acting U.S. Attorney O'Neill in Tampa. And O'Neill got in touch with the FBI and the Florida Department of Law Enforcement.

Our investigation revealed that the couple used the CDs—which were also in Asia Oropeza's name—as collateral when applying for two separate mortgage loans, and then once the CDs matured, they used the funds to pay off those loans.

**Outcome.** Asia Oropeza pled guilty to fraud, while her husband was later convicted at trial. They were ordered to pay Markus restitution, had their real estate holdings seized, and received prison terms.

And last month in Tampa, during a press conference attended by investigators and prosecutors who worked the case, the 25-year-old Markus, who works as a concert stage hand in New York, received full restitution—a check for $409,662.07. He told the press that receiving the money gave him "a new lease on life."

Special Agent Kelly says that the investigation brought him and everyone else involved a great deal of satisfaction. "Cases like this," he explained, "show us what kind of impact our work actually has, and that's what keeps us out there doing it every day."

# Buying a Car Online?
## Read This First

You can buy almost anything over the Internet—including clothes, a pizza, music, a hotel room, even a car. And while most transactions are conducted lawfully and securely, there are instances when criminals insert themselves into the marketplace, hoping to trick potential victims into falling for one of their scams.

Today, the FBI's Internet Crime Complaint Center (IC3) issued an alert about a specific type of cyber scam that targets consumers looking to buy vehicles online.

**How the scam works.** While there are variations, here's a basic description: consumers find a vehicle they like—often at a below-market price—on a legitimate website. The buyer contacts the seller, usually through an e-mail address in the ad, to indicate their interest. The seller responds via e-mail, often with a hard-luck story about why they want to sell the vehicle and at such a good price.

In the e-mail, the seller asks the buyer to move the transaction to the website of another online company…for security reasons…and then offers a buyer protection plan in the name of a major Internet company (e.g., eBay). Through the new website, the buyer receives an invoice and is instructed to wire the funds for the vehicle to an account somewhere. In a new twist, sometimes the criminals pose as company representatives in a live chat to answer questions from buyers.

Once the funds are wired, the buyer may be asked by the seller to fax a receipt to show that the transaction has taken place. And then the seller and buyer agree upon a time for the delivery of the vehicle.

**What actually happens:** The ad the consumer sees is either completely phony or was hijacked from another website. The buyer is asked to move from a legitimate website to a spoofed website, where it's easier for the criminal to conduct business. The buyer protection plan offered as part of the deal is bogus. And the buyer is asked to fax the seller proof of the transaction so the crooks know when the funds are available for stealing.

And by the time buyers realize they've been scammed, the criminals—and the money—are long gone.


**Red flags for consumers:**

- Cars are advertised at too-good-to-be true prices;
- Sellers want to move transactions from the original website to another site;
- Sellers claim that a buyer protection program offered by a major Internet company covers an auto transaction conducted outside that company's website;
- Sellers refuse to meet in person or allow potential buyers to inspect the car ahead of time;
- Sellers who say they want to sell the car because they're in the U.S. military about to be deployed, are moving, the car belonged to someone who recently died, or a similar story;
- Sellers who ask for funds to be wired ahead of time.

**Number of complaints.** From 2008 through 2010, IC3 has received nearly 14,000 complaints from consumers who have been victimized, or at least targeted, by these scams. Of the victims who actually lost money, the total dollar amount is staggering: nearly $44.5 million.

If you think you've been victimized by an online auto scam, file a complaint with IC3. Once complaints are received and analyzed, IC3 forwards them as appropriate to a local, state, or federal law enforcement agency.


# Intelligence Analysts

## Part 1: Central to the Mission

The FBI has always relied on gathering and using intelligence to solve crimes and to keep the country safe. That was true when we were hunting Nazi spies on U.S. soil during World War II, and it was true when agents were dismantling the Mafia's Five Families in New York decades later. But 9/11 made it clear that our intelligence efforts needed to change—and change quickly—to meet the global threat of terrorism.

**In the 10 years since 9/11, the Bureau has transformed itself from an organization that uses intelligence to one that is defined by it. Nowhere is that more apparent than in our intelligence analyst program.**

Prior to 9/11, there were approximately 1,000 intelligence analysts (IAs) in the FBI. Today, there are triple that number. "Now, instead of just agents working cases, there are intelligence analysts working right alongside them," said Amy Pepper, a senior intelligence manager. "And that's across the entire spectrum of FBI programs."

That means in criminal cases as well as national security matters, IAs are on the front lines—analyzing and disseminating actionable intelligence that enables the FBI and our domestic and international partners to get ahead of existing and emerging threats.

The Bureau's transformation into an intelligence-driven organization has been successful, Pepper explained, "because our leadership understood that the change was necessary and that it was simply the right thing to do to mitigate the threats the country faces."

The Directorate of Intelligence (DI), established in 2005, is a key component of the FBI's National Security Branch and manages all Bureau intelligence activities.

"With regards to intelligence, we're not doing anything today that we didn't do before 9/11, but it wasn't systematic then, and now it is," said Dina Corsi, a senior manager in the DI and a veteran analyst who specialized in counterterrorism work.

Prior to 9/11, Corsi said, "IAs could always do what was needed, but there was no system-wide program across the FBI as there is now, with formal training, standardized intelligence products, and clear-cut career paths for analysts. In those days," she recalled, "the efforts of IAs, while considerable, existed in pockets."

**Now, with the entire intelligence analyst program administered under the DI, all areas of the Bureau can leverage intelligence resources, and those resources can be used much more broadly and efficiently to connect programs and investigations.** That helps agents in the field and underscores the value and importance of IAs throughout the FBI.

"The scope and topic of particular intelligence needs may be different for agents in Portland and in Miami," Corsi explained, "but now the process and the training are the same, which makes information that much more accessible and analysis more consistent across the organization."

New Bureau analysts attend the 10-week Intelligence Basic Course at our Quantico training facility, where they learn critical thinking skills, research and analysis techniques, and communications skills, as well as how to produce a variety of intelligence reports and briefings.

Within the U.S. intelligence community, Pepper said, "the FBI is no longer seen as just a law enforcement agency but also a national security intelligence entity. And in the intelligence community, we are one of the few agencies that not only have the responsibility to gather intelligence, but to act on it as well."

# Intelligence Analysts

## Part 2: The Subject Matter Experts

Intelligence analysts—IAs in Bureau parlance—are involved in nearly every aspect of FBI operations in every corner of the globe. And in the decade since 9/11, their role has continued to expand.

**"Even though analysts don't carry weapons or arrest individuals, there is a growing recognition that what we bring to the table is extremely valuable and that we are an integral part of the team," said Sally Rall, an IA who works in one of our regional intelligence groups in Sacramento.**

Analysts begin their FBI training with the 10-week Intelligence Basic Course to learn fundamental skills. Soon after they begin to specialize in one of three distinct analytic areas: strategic, tactical, or collection/reporting. Rall, for example, is a tactical analyst who works on domestic terrorism matters.

"Tactical IAs are less big picture and more boots on the ground," she explained. "If an agent needs to get in the car and go arrest someone before that person hurts somebody, the agent can call an IA for vital information—information that can save lives."

**Strategic analysts, on the other hand, work on longer-term threats on a broader scale.** Whereas a tactical IA might be focused on a gang case in a particular area, the strategic IA might be looking at the gang's activities from a national or transnational perspective.

"Strategic analysis is less about a specific case and more about understanding what we know and what we don't know about a threat," said Marita Cook, a strategic IA in our Geospatial Intelligence Unit at Headquarters. "We look at threats, vulnerabilities, and gaps in our knowledge for every FBI program. Often, there is so much raw information—from cases, sources, and other data—that it's difficult to bring it all together into one clear picture," Cook added. "Our job is to provide clarity."

IAs who work in the collection/reporting discipline are generally responsible for understanding the Bureau's intelligence collection capabilities and how they integrate across the FBI and with the entire U.S. intelligence community. They also ensure that information is disseminated in a timely manner.

"In collection, we're not evaluating the why of the case or even the threat—we're telling you how we're positioned to collect against it and what capabilities we have—or need—to fill the gaps," said Dina Corsi, chief of the Domain Collection Operations Support Section in the Directorate of Intelligence.

**The goal, Corsi said, is to build collection and reporting capabilities and make the results available to all programs across the Bureau.** "So if you are working in counterintelligence and the Criminal Division might have assets you could use, you would be aware of that and be able to leverage it. Our job is to streamline the intelligence process."

Like many of her IA colleagues, Rall was motivated to join the Bureau to fight terrorism after the 9/11 attacks. She is impressed with the dedication and professionalism of her fellow analysts.

"I have met incredibly brilliant people who are analysts here," said Rall, who has a doctorate in psychology. "There are lawyers, scientists, people who are multilingual, national and international experts in their fields with priceless institutional knowledge going back over 20 years. It's an honor to work in this environment."

# Intelligence Analysts

## Part 3: A Rewarding Career

In the decade since the 9/11 attacks, the FBI's intelligence program has tripled in size, and our analysts work around the world—from the war zone in Afghanistan to the White House Situation Room—to help keep the country safe.

**Behind the scenes, Bureau administrators are working hard to make the FBI a great career choice for intelligence professionals by defining career paths, offering advanced training, and establishing senior-level positions within the organization.**

Tonya Ugoretz, the Bureau's chief intelligence officer, manages our senior intelligence officers (SIOs), a group of highly skilled professionals whose job description did not exist 10 years ago. "Certainly 9/11 was part of the reason for creating the SIO corps," Ugoretz said. "We needed an entity that transcended the stove pipes of specific program areas, and we wanted to provide analysts with senior positions they could aspire to. Developing this career ladder helps us increase the opportunities for analysts, and it deepens our bench analytically."

Currently, there are approximately a dozen SIOs whose expertise covers all FBI investigative programs, from counterterrorism and counterintelligence to criminal matters. Some SIOs are assigned geographic territories—where many criminal and national security investigations overlap—and are acknowledged experts on key areas around the world.

"SIOs look at threats and issues from a very broad perspective," Ugoretz explained. "Our focus is more big-picture than day to day cases. SIOs regularly give advice and counsel to our senior leadership, so we are always looking at what we know and also what we don't know."

**That means SIOs are required to understand current threats but are also responsible for "looking over the horizon to see what we should be anticipating," Ugoretz added.** "What do we know today? What should we be thinking about for the future? What are the risks and opportunities that present themselves? These are the issues tailor-made for senior intelligence officers."

SIOs also serve as a bridge between the FBI and the wider intelligence community, making sure that the FBI's perspective is factored into the entire intelligence community's thinking—and making sure the intelligence community's perspective is known to decision makers inside the Bureau. SIOs perform a similar liaison role with the academic community as well.

These senior analysts usually come from the ranks of career intelligence professionals and have significant subject matter expertise in their chosen field. "My section mainly focuses on intelligence for the Bureau's executive decision-makers," Ugoretz said. "Our role is to make sure leadership is aware of all the information and analysis we are generating Bureau-wide. The products we provide can ultimately factor into decisions made at the highest levels of government."

The concept of senior intelligence officers is a relatively new one to the FBI, Ugoretz said. "So far, the more interaction our workforce has with SIOs, the more they see the value of the position. We look forward to building on that success."

# FBI in Montana

## Part 1: In Resident Agencies, Agents are 'Jacks of All Trades'

In the early days of the FBI under J. Edgar Hoover, popular lore has it that agents who botched a job risked exile to the Bureau's remote field office in Butte, Montana. The field office closed in 1989, but the FBI still sends plenty of agents to the Big Sky state. It's not a punitive measure, but a concerted effort to tackle the same threats confronting the rest of the country.

**"If you think this is a sleepy little burg, think again," says Scott Cruse, an assistant special agent in charge in Helena, one of 10 satellite offices, or resident agencies, in Montana under the governance of the Salt Lake City Field Office**, which also covers Utah and Idaho. Priorities here largely mirror those of every other field office: fraud, corruption, cyber scams, child pornography, terrorism, criminal networks. "We may not have the large enterprises in Montana, but we work it up the chain," Cruse says. "We follow that thread."

Oftentimes, the thread extends well beyond the state's expansive borders. In one recent case, an agent in Helena working with local police peeled back the seedy layers of a child pornography web spanning at least five states. In another case, an agent in Bozeman unraveled a local conman's ruse to trick investors into pouring millions into a fictitious gold-mining scheme. The cases, which we will feature in the coming days on FBI.gov, illustrate how despite the region's relative remoteness it is not immune to the prevailing threats of the modern era.

**"It's not a small world for us anymore," says Special Agent Greg Rice**, who works in the Bozeman resident agency. "We tend to find a lot of cases that are connected to other states or even foreign nationalities." In one such case, a local bank received a fax on what appeared to be the letterhead of a local business. The fax actually originated in Russia, instructing the teller to transfer $50,000 to a foreign account.

"There's a lot of wealth here," Rice says. "The people are very nice. They're very trusting."

The FBI has 56 field offices and about 380 resident agencies across the U.S. While in the larger field offices agents might work on terrorism or white-collar squads, agents like Rice in the small resident agencies have to be generalists—capable of working any case anytime.


**The FBI has 10 satellite offices, or resident agencies, in Montana under the governance of the Salt Lake City Field Office in Utah.**

"You have to learn to handle them all," says Rice. "If people are calling in about fraud you've got to deal with it. You can't wait for the fraud guy to come back."

The Montana offices support each other on large operations, but individual cases are generally handled locally. Agents in the Kalispell office in Northwest Montana, for example, might focus more heavily on domestic terrorist threats, while in Bozeman and Billings the agents might be tracing the interstate flow of drugs or cyber scams. The 600-mile border with Canada also presents special challenges.

**Agent Cruse says it takes a special type of agent to work in a resident agency, or RA. "You have to be a jack of all trades,"** he says. "You've got to be willing to work long, odd hours, you've got to be able to get along with the local police, you've got to be diplomatic, and you've got to have a tough skin."

"When you're in a small RA," Agent Rice adds, "you are the face of the FBI."


# FBI in Montana

## Part 2: Bozeman Fraud Case Shows 'It's Not a Small World'

Special Agent Greg Rice asked questions and scribbled notes as the woman on the phone detailed why she thought she was being scammed.

Did she have records, receipts, account numbers? Was she still on good terms with the suspected scammer? From the moment he picked up the phone in the Bozeman Resident Agency, Rice was laying the groundwork for a potential case. A day earlier, he took two similar calls.

"A lot of my time is dedicated to working fraud," says Rice, who was an agent in Las Vegas for eight years before moving to Bozeman six years ago. "We don't take everything that comes in the door. But there's a lot to choose from."

**In resident agencies, which are slimmed-down satellites of the Bureau's 56 field offices, case agents are the face of the FBI for local police departments, community leaders, and the public.** In the smaller offices like Rice's in Bozeman—an affluent college town surrounded by farms, ranches, and retired millionaires—agents field complaints of all stripes and vet which ones cross the threshold for federal involvement. One such case, an Internet fraud scam in 2009 that reached victims as far afield as Florida and Texas, illustrates how complaints like the phone calls Rice picked up in early July can bloom into full-blown investigations.

In that case, a woman in Florida called Rice to report that she sent $225,000 to a Bozeman man who claimed he had a stockpile of unrefined gold and was looking for investors to finance refineries. He promised big returns. When that didn't materialize, the investor got suspicious.

"She became angry over the investment and called us," Rice says. When he followed the money and confirmed their suspect, Carl Estep, wasn't putting his investors' money where he'd promised, Rice set up a sting. Only this time, he would play the patsy. Working with a female FBI agent from the Billings resident agency, Rice staged a ruse to pose as husband-and-wife investors who wanted a piece of Estep's venture. They set up a meeting at the airport in Bozeman to make it seem as though they had just arrived from Chicago.

"We came off the plane, we met him, and we sat down in the coffee shop," Rice says. "I wore a camera and a wire—and he pitched the whole deal to me, the exact same deal that he pitched to the victim."

It didn't end there, though. Estep then escorted the would-be investors to a warehouse where he showed them stacks of barrels that he claimed each contained about 1,200 ounces of unrefined gold.

"It was the exact same pattern as what he did with these other people," Rice says. "He flew them out here. He took them to the warehouse. He showed them the barrels stacked up. All he'd done was get his hands on a bunch of barrels with gravel in them. The rest was easy for him."

The FBI tested samples from the barrels—which didn't contain gold—and identified more victims, including the provider of the warehouse. Confronted with the evidence, Estep pleaded guilty in January and is now serving a four-year sentence.

**"It's not a small world for us anymore,"** says Rice, an Idaho native, describing how even this once-remote area is no longer so, due in part to the Internet.

# Health Care Fraud Takedown

## Targets $295 Million in False Medicare Claims

In Houston, two individuals were charged today with Medicare fraud schemes involving $62 million in false claims for home health care and durable medical equipment. According to the indictment, one of the defendants sold Medicare beneficiary information to 100 different Houston-area home health care agencies, and the agencies used that information to bill Medicare for services that were unnecessary or not even provided.

**But that's just the tip of today's enforcement iceberg:** this afternoon, Attorney General Eric Holder, FBI Executive Assistant Director Shawn Henry, and other officials announced a nationwide takedown that took place over the past week involving Medicare Fraud Strike Force operations in seven other cities as well—Baton Rouge, Brooklyn, Chicago, Dallas, Detroit, Los Angeles, and Miami. A total of 91 individuals were charged with various Medicare fraud-related offenses, including fraudulent billings of approximately $295 million, the largest amount in phony claims involved in a single takedown in Strike Force history.

**The Medicare Fraud Strike Force, coordinated jointly by the Department of Justice (DOJ) and the Department of Health and Human Services (HHS), is a multi-agency team** of federal, state, and local investigators who combat Medicare fraud by analyzing data about the problem and putting an increased focus on community policing. The strike force is part of the Health Care Fraud Prevention and Enforcement Action Team (HEAT), another joint DOJ-HHS initiative that works to prevent and deter fraud and enforce current anti-fraud laws. The strike force currently operates in nine U.S. cities (the eight cities mentioned previously, plus Tampa) in areas victimized by high levels of health care fraud.

**Other cases announced today include:**

- In Miami, 45 individuals—including a doctor and a nurse—were charged for their participation in various fraud schemes involving a total of $159 million in fraudulent Medicare billings in the areas of home health care, mental health services, occupational and physical therapy, durable medical equipment, and HIV infusion.

**FBI Executive Assistant Director Shawn Henry, left, is joined by Attorney General Eric Holder and HHS Secretary Kathleen Sebelius in announcing a nationwide Medicare fraud takedown operation.**

- In Los Angeles, six defendants—including one doctor—were charged for their roles in schemes to defraud Medicare of more than $10.7 million.
- In Brooklyn, three defendants—including two doctors—were charged in a fraud scheme involving more than $3.4 million in false claims for medically unnecessary physical therapy.
- In Detroit, 18 additional defendants—including doctors, nurses, clinic operators, and other health care professionals—were charged for schemes involving an additional $28 million in false billing.

**In addition to our role on the Medicare Fraud Strike Force, the FBI also operates health care fraud task forces or working groups in all 56 of our field offices.** Hundreds of agents and analysts—using intelligence to identify emerging schemes and tactics—are currently working more than 2,600 health care fraud investigations.

Nearly 70 percent of these cases involve government-sponsored programs, like Medicare, since the Bureau is the primary investigative agency with jurisdiction over federal insurance programs. But we also have primary investigative jurisdiction over private insurance programs, and we work closely with private insurers to address threats and fraud directed towards these programs.

**Taking part in this takedown were more than 400 law enforcement personnel from the FBI, HHS-Office of Inspector General, multiple Medicare fraud control units, and state and local law enforcement agencies.**


# FBI in Montana

## Part 3: Online Operation Reveals Network of Predators

When Kyle Burris struck up a conversation with a single mother of two young daughters in an online chat forum in 2008, he could not have imagined the direction it would take. What he thought was going to happen was this: he'd send the Montana woman some images of child pornography and she would reciprocate with pictures of her own kids being molested. So sure was Burris that this scenario would play out, he e-mailed images to the woman during their very first chat, and over the next few weeks began making plans to travel from New York to Montana.

What he did not expect was that the "woman" was Special Agent Kevin Damuth of the FBI's resident agency in Helena, one of 10 Montana satellite offices under the umbrella of the Salt Lake City Field Office in Utah. Like most agents in the FBI's approximately 380 resident agencies, Damuth is a generalist, equally aplomb at handling white-collar and violent crimes, fraud, and cyber crimes. In recent years, however, working with the Helena Police Department on the Montana Internet Crimes Against Children (ICAC) Task Force, he has developed a unique skill in snaring child pornographers, whose use of the Internet makes rural Montana as susceptible to predators as any big city.

**"That's the thing about Montana," says Damuth, an agent of almost 13 years, most of them in Helena. "Not only are things happening here, there's almost always a nexus outside of the state."**

In the Burris case, agents from Helena and the ICAC Task Force in Buffalo, New York arrested the 40-year-old man in December 2008. He was prosecuted in Montana, where authorities received consent to take over his online identity and link up his circle of acquaintances. This is where a larger web came into focus.

"It spun off across the country," Damuth says.

Helena Police Department Detective Bryan Fischer assumed Burris' identity and quickly honed in on Russel Bradney of Sacramento. Under the guise of Burris, Det. Fischer traded messages with Bradney and collected evidence. Meanwhile, the FBI in Sacramento was already making a case on Bradney and discovered he was trading child pornography with Thomas Elgert of New Jersey. Agents and ICAC officers in Sacramento moved on Bradney. Then Agent Damuth in Montana took over Bradney's identity, continuing the correspondence with Elgert in New Jersey and another man, Anthony Richards, in Maine.

At this point, Det. Fisher was still undercover as Kyle Burris, and Agent Damuth was continuing the personas of both Bradney and the single mother in Montana. When Elgert got word from Bradney's account about a Montana woman and her two daughters, he expressed interest.

"I was communicating with him at both ends," Agent Damuth recalls.

In March 2009, the FBI and ICAC officers arrested Anthony Richards in Maine. Damuth and agents in Newark arrested Elgert two months later, but not before linking him to yet another child pornographer, Ted Girdner, in California. He was arrested in August 2009.

**A cadre of state and federal officers and agents on the Innocent Images National Initiative Task Force and the Montana ICAC Task Force played essential roles**, Damuth says. All the suspects received hefty prison sentences. Meanwhile, untold numbers of victims remain unidentified, the exact origins of their images unknown. Montana has its own share of homegrown cases, but Damuth and Fisher are never surprised when a trail leads far beyond their borders.

"When we get stuff like this it can go wherever," says Det. Fischer. Adds Damuth, "Nothing surprises me anymore."

# Surrogacy Scam

## Played on Emotions of Vulnerable Victims

It's a shocking tale.

Three women recently pled guilty in San Diego, admitting to taking part in a scheme to illegally create an inventory of babies to sell to unwitting would-be parents for fees of between $100,000 and $150,000 each.

The three took advantage of couples who desperately wanted children, offering them seemingly legitimate surrogacy situations. They also took advantage of women recruited as "gestational carriers" to carry pregnancies to term after having embryos transferred to their uteruses.

The defendants in this case included two lawyers who specialized in reproductive law: Theresa Erickson, a well-known California attorney, and Hilary Neiman, who operated an adoption/surrogacy agency in Maryland. The third conspirator was Carla Chambers of Nevada, who served as the "surrogacy facilitator." Together, they circumvented surrogacy regulations that say contracts between surrogates and intended parents must be executed **before** a pregnancy occurs…and lied to surrogates, intended parents, and the California family court.

**Here's how the scam worked:** Chambers admitted visiting adoption/surrogacy-themed online chat rooms and forums in search of surrogates and parents. Erickson and Neiman also used their own sterling reputations to legitimize the scheme.

Surrogates were made to travel to Ukraine in Eastern Europe to become implanted with embryos derived from anonymous donors—Chambers usually made all the arrangements—with the promise that they would be compensated by the intended parents. The women were led to believe that they were participating in legal surrogacy arrangements and that there was a waiting list of potential parents for the babies. They also had to agree to give birth in California.

They were promised quick matches with intended parents, but the co-conspirators usually waited until the second or even third trimester of the pregnancies before seeking parents. Neiman and Erickson then drafted contracts between the surrogates and intended parents, well after the time frame required by law.

The hopeful couples were told the unborn babies were the result of legitimate surrogacy arrangements, but the

original intended parents had backed out. They were offered the opportunity to "assume" the non-existent surrogacy agreement. The parents would hand over between $100,000 and $150,000 to the defendants, but less than half of that went to the surrogate—Erickson, Neiman, and Chambers pocketed the rest.

**The defendants typically used the Internet to recruit, solicit, and communicate with surrogates and intended parents. Most of the surrogates and parents lived outside of California.**

One of the most critical aspects of the scheme involved Erickson filing fraudulent documents in California court stating that a surrogacy agreement had been in place from the start and asking for what's called a "pre-birth judgment" that would establish parental rights. That way, under California law, the names of the intended parents could be placed on the birth certificate when the baby was born.

The scam was uncovered when one of the surrogates, nearly seven months pregnant, was worried that parents hadn't been found for the baby she was carrying. She contacted a lawyer, who then contacted the FBI's San Diego office.


# The NCFTA

## Combining Forces to Fight Cyber Crime

Long before it was acknowledged to be a significant criminal and national security threat, the FBI established a forward-looking organization to proactively address the issue of cyber crime.

**Since its creation in 1997, the National Cyber Forensics and Training Alliance (NCFTA), based in Pittsburgh, has become an international model for bringing together law enforcement, private industry, and academia to share information to stop emerging cyber threats and mitigate existing ones.**

"The exchange of strategic and threat intelligence is really the bread and butter of the NCFTA," said Special Agent Eric Strom, who heads the FBI unit—the Cyber Initiative and Resource Fusion Unit (CIRFU)—assigned to the NCFTA. "The success of this effort at every level comes down to the free flow of information among our partners."

When the nonprofit NCFTA was established, the biggest threat to industry was from spam—those annoying unsolicited e-mails that fill up inboxes. Today, the organization deals with malicious computer viruses, stock manipulation schemes, telecommunication scams, and other financial frauds perpetrated by organized crime groups who cause billions of dollars in losses to companies and consumers.

**The NCFTA essentially works as an early-warning system.** If investigators for a major banking institution, for example, notice a new kind of malware attacking their network, they immediately pass that information to other NCFTA members.

Alliance members—many have staff permanently located at the NCFTA—then develop strategies to mitigate the threat. FBI agents and analysts from CIRFU, also located at NCFTA headquarters, use that information to open or further existing FBI investigations, often in concert with law enforcement partners around the world.

"Cyber crime has changed so much since those early days of spamming," Strom said. "And the threat continues to evolve globally, which is why the NCFTA's work is so critical to both business and law enforcement."

The organization draws its intelligence from hundreds of private-sector members, Carnegie Mellon University's Computer Emergency Response Team (CERT), and the FBI's Internet Crime Complaint Center (IC3). That extensive knowledge base has helped CIRFU play a key role in some of the FBI's most significant cyber cases in the past several years.

**Training is another important role of the NCFTA.** Last year, an international internship program was held in which cyber investigators from Germany, Great Britain, Australia, the Netherlands, Lithuania, and the Ukraine came to the alliance headquarters for 90 days to share knowledge, build relationships, and help with each others' investigations.

"Working with CIRFU and the NCFTA makes our cooperation very direct," said Mirko Manske, a cyber investigator for the German Federal Criminal Police. "We can work in real time, sharing information and moving our cases forward. That is one of the biggest gains for us."

Manske added, "If I need a contact in the U.S., I reach out to CIRFU, and they help me immediately. And we do the same for them. Basically we are opening doors for each other."

When it comes to the global reach of cyber crime, Manske said, "The FBI gets it. They realize that no one organization can succeed by itself. CIRFU started all of this," he added. "The unit is one of the reasons the FBI is recognized as one of the worldwide leaders in the fight against cyber crime."

# Latest Crime Statistics

## Volumes Continue to Fall

The incidence of crime nationwide decreased again, according to our just released *Crime in the United States* report. Overall, the estimated volume of violent crimes in 2010 dropped 6 percent compared to the 2009 figure, the fourth consecutive year it has declined. For the eighth consecutive year, the volume of property crimes went down as well—2.7 percent.

**The report was compiled from data submitted to us by more than 18,000 city, county, university and college, state, tribal, and federal law enforcement agencies from around the nation.** It contains information on the number of reported murders and non-negligent manslaughters, forcible rapes, robberies, aggravated assaults, burglaries, larceny-thefts, motor vehicle thefts, and arsons.

Violent crime offenses were down across the board—the largest decrease was robbery, down 10.0 percent. Property crime offenses went down as well—the largest decline, 7.4 percent, was for motor vehicle thefts.

**Here are some highlights from *Crime in the United States, 2010*:**

- Total number of crimes reported: 10,329,135 (1,246,248 violent crimes and 9,082,887 property crimes);
- Most common violent crime: aggravated assault (62.5 percent of all violent crimes during 2010);
- Most common property crime: larceny-theft (68.2 percent of all property crimes during 2010);
- Top three crimes for which law enforcement reported arrests: drug abuse violations (1,638,846), driving while intoxicated (1,412,223), and larceny-theft (1,271,410);
- Total number of arrests, excluding traffic violations: 13,120,947, including 552,077 for violent crimes and 1,643,962 for property crimes (the number of arrests doesn't reflect the number of individuals arrested—some individuals may have been arrested more than once);
- Most common characteristics of arrestees: 74.5 percent of arrestees were male, and 69.4 percent of arrestees were white;


- How often firearms were used in crimes: in 67.5 percent of reported murders, 41.4 percent of reported robberies, and 20.6 percent of aggravated assaults; and
- Total losses for victims of property crimes, excluding arsons: an estimated $15.7 billion.

**Beyond the crime count.** The report contains what's called "expanded offense data." This information involves additional details about some of the crimes—i.e., type of weapon used; locations of robberies; type or value of items stolen; and for the offense of murder, the age, sex, and race of victims and offenders, and, if known, the relationship of the victim to the offender.

It also contains arrest data on the above crimes, plus about 20 other offenses, including forgery/counterfeiting, fraud, gambling, weapons violations, drug violations, sex offenses, and driving under the influence.

You can browse through the statistics contained in the report and choose particular information you'd like to focus on—like national data, regional data, state totals, reporting agencies, cities and counties grouped by populations, and statistics from certain metropolitan areas.

**We caution against drawing any kind of conclusions from the report by making direct comparisons between cities.** Valid assessments are only possible with an understanding of various factors affecting each jurisdiction.

According to FBI Director Robert Mueller, *Crime in the United States* can provide "valuable insight into the nature and volume of crime in small and large communities alike." It can also "offer a picture that experts can study, and as a result, produce new strategies or improve current methods of combating crime."

Left: A cache of guns seized from militia extremists

# Domestic Terrorism

## Focus on Militia Extremism

Last March, nine members of an extremist militia group were charged in Michigan with seditious conspiracy and attempted use of weapons of mass destruction in connection with an alleged plot to attack law enforcement and spark an uprising against the government.

According to the federal indictment, the nine individuals planned to kill a law enforcement officer and then use bombs to attack the caravan of cars taking part in the subsequent funeral procession, hoping that this violence would incite a larger armed conflict with authorities. Fortunately, the FBI and the Michigan State Police intervened and took the subjects into custody before they could carry out their alleged plot.

**It's just one example of the dangers posed by so-called militia extremists—the latest topic in our series to educate the nation on domestic terror threats that the FBI investigates today.** Previous stories have focused on anarchist extremists, eco-terrorists/animal rights extremists, lone offenders, and sovereign citizen extremists.

**Who they are.** Like many domestic terrorism groups, militia extremists are anti-government. What sets them apart is that they're often organized into paramilitary groups that follow a military-style rank hierarchy. They tend to stockpile illegal weapons and ammunition, trying illegally to get their hands on fully automatic firearms or attempting to convert weapons to fully automatic. They also try to buy or manufacture improvised explosive devices and typically engage in wilderness, survival, or other paramilitary training.

**Who and what they target.** They usually go after the government itself—including law enforcement personnel, representatives of the courts, and other public officials, along with government buildings. When caught, most militia extremists are charged with weapons, explosives, and/or conspiracy violations.

**What they believe in.** Many militia extremists view themselves as protecting the U.S. Constitution, other U.S. laws, or their own individual liberties. They believe that the Constitution grants citizens the power to take back the federal government by force or violence if they feel it's necessary. They oppose gun control efforts and fear the widespread disarming of Americans by the federal government.

Militia extremists often subscribe to various conspiracy theories regarding government. One of their primary theories is that the United Nations—which they refer to as the New World Order, or NWO—has the right to use its military forces anywhere in the world (it doesn't, of course). The extremists often train and prepare for what they foresee as an inevitable invasion of the U.S. by United Nations forces. Many militia extremists also wrongly believe that the federal government will relocate citizens to camps controlled by the Federal Emergency Management Agency, or force them to undergo vaccinations.

**One important note:** simply espousing anti-government rhetoric is not against the law. However, seeking to advance that ideology through force or violence is illegal, and that's when the FBI and law enforcement become involved.

**What is the FBI doing to combat the militia extremism threat?** In addition to our lawful use of sophisticated investigative techniques, we've expanded our work with other federal agencies such as the Bureau of Alcohol, Tobacco, Firearms, and Explosives and with our state and local partners. And we use intelligence and analysis to help identify gaps in our knowledge, emerging tactics and trends, and effective investigative strategies.

As always, the combination of intelligence, coordinated law enforcement efforts, and an informed public is the most effective way to counter the threats posed by domestic extremists.

# Making a Point About Lasers

## Illegal Use of Devices a Serious Crime

Justin Stouder was aiming a laser pointer at a distant tower from his suburban St. Louis yard one April evening in 2010 when a police helicopter appeared in his line of sight more than a mile away.

**At the time, the 24-year-old had no idea that his decision to point the laser at the helicopter was a federal felony—or that the beam of light might have serious consequences for the pilot and his crew.**

"It's equivalent to a flash of a camera if you were in a pitch black car at night," said St. Louis Metropolitan Police Officer Doug Reinholz, the pilot on patrol that night when Stouder's green hand-held laser "painted" his cockpit. "It's a temporary blinding to the pilot," he said during a recent news conference highlighting the danger of lasers directed at airplanes and helicopters.

Interfering with the operation of an aircraft is a crime punishable by a maximum of 20 years in prison and a $250,000 fine, and laser incidents are on the rise. Since the FBI and Federal Aviation Administration (FAA) began keeping records of laser events in 2004, "there has been an exponential increase every year," said Tim Childs from the Federal Air Marshal Service, who serves as a liaison officer with the Bureau on laser issues.

In 2009, there were 1,489 laser events logged with the FAA—that is, pilots reporting that their cockpits were illuminated by the devices. The following year, that figure had nearly doubled to 2,836, an average of more than seven incidents every day of the year. And the overwhelming number of the incidents involved green lasers—especially dangerous because the human eye is most susceptible to damage from the yellow-green light spectrum.

Hand-held lasers—about the size of fountain pens—are used legitimately by astronomy hobbyists and in industrial applications. Anyone can purchase one, and technology has made them inexpensive and more powerful. Lasers costing as little as $1 can have ranges of two miles—strong enough to target a variety of aircraft.

**And what appears as a dot of light on the ground can illuminate an entire cockpit, disorienting a pilot or causing temporarily blindness.** That's because the farther the beam travels the more spread out it becomes. "At 500 feet," Childs said, "that two-centimeter dot you see on your wall can be six feet wide." To date, no aircraft have been lost as a result of laser incidents, he added, but there have been eye injuries, and perpetrators have gone to jail.

**What appears as a dot of light on the ground can illuminate an entire cockpit, disorienting a pilot or causing temporary blindness.**

Those responsible for "lasering" aircraft fit two general profiles, Childs explained. "Consistently, it's either minors with no criminal history or older men with criminal records." The teens are usually curious or fall victim to peer pressure, Childs said. The older men simply have a reckless disregard for the safety of others. There are also intentional acts of laser pointing by human traffickers or drug runners seeking to thwart airborne surveillance, Childs added.

As for Justin Stouder, the helicopter pilot he lasered helped guide police to his house, where he was arrested minutes after the incident.

"I had no idea it illuminated the whole cockpit and blinded everybody inside," Stouder said during the news conference. He offered a public apology and volunteered to tell his story in the hopes of educating the public about the dangers of laser pointing. "It was really a selfish mistake," he said of his actions.

Left: Amy and Tom Wales issue a plea for information about their father's 2001 murder in Seattle.

# Help Us Find a Killer

## Media Campaign Marks Anniversary of Prosecutor's Murder

It has been nearly 10 years since a killer stood outside the Seattle home of Tom Wales and fired several shots from a handgun through a basement window, killing the assistant U.S. attorney and father of two while he worked at his desk.

**Since that time, the FBI and our law enforcement partners have dedicated themselves to finding those responsible for the murder. Now, as the 10th anniversary of the killing approaches on October 11, we are announcing a new media campaign to again ask for the public's assistance.**

"This is an active case in which we are constantly and aggressively pursuing leads," said Greg Fowler, the FBI inspector in charge of the task force investigating the murder. "Information is the key," Fowler added, "and the better the information, the greater the chance of finding those responsible."

**Wales, a prosecutor who specialized in white-collar crime cases, was shot at 10:40 p.m. It has been reported that a lone male suspect was observed leaving the scene.**

"We know information about the crime is still out there," Fowler said. "We know there are people who—because of fear, doubt, or other reasons—have not yet come forward. Regardless of the reasons, now is the time to come forward. Now is the time to tell us what you know. Now is the time to help us solve this crime."

During the next few weeks, residents in the Seattle region will see and hear a variety of print, broadcast, and billboard advertisements regarding the Wales investigation and the reward of up to $1 million for information leading to the arrest and conviction of those responsible. In addition, detailed information about the case will be available on our website and our social media outlets, including Facebook.

"There are those who may not even know their information is important," Fowler said, explaining the need for the media campaign. "Something seen, something heard, something out of place, something unusual—even the smallest clue may help."

Special Agent Russ Fox, who has been supervising the investigation for the past two years, added that the 10th anniversary of the murder is a natural point to "renew the public's interest in the investigation." Fox noted that the murder took place exactly one month after the 9/11 terrorist attacks, which should help people remember that time period.

**Fox acknowledged that the case has special significance because Wales was a federal prosecutor and a partner to law enforcement. "But he was also a neighbor, a father, and a member of our community."**

The FBI, the Seattle Police Department, the King County Prosecuting Attorney's Office, and the Department of Justice—which form the Seattle Prosecutor Murder Task Force—"are still fully committed to this case," Fox said.

"The murder of Tom Wales was more than a single act of violence against an individual," Fowler added. "It was a crime that impacted many, but no one more than his family. Tom Wales left behind a legacy and a life that cannot be replaced. We remain confident that, with the public's help, we will find those responsible and bring them to justice."

If you have any information about the case, there are three ways you can contact the FBI, all of which are confidential:

- Call (206) 622-0460;
- E-mail walestips@ic.fbi.gov; or
- Send a letter to P.O. Box 2755, Seattle, WA 98111.

# Protecting our Children

## Technology, Partnerships Work Hand in Hand

Investigators dedicated to rescuing child victims of sexual abuse and arresting those who traffic in child pornography are often faced with the difficult and time-consuming task of analyzing hundreds of thousands of illicit images traded online.

**That painstaking work is critical to identifying victims and their abusers, however, and members of our Digital Analysis and Research Center (DARC)—part of the FBI's Innocent Images National Initiative—use a mix of sophisticated computer tools and domestic and international partnerships to get the job done.**

DARC personnel, who analyze digital evidence in the most significant online child exploitation cases, are currently testing a software tool called the Child Exploitation Tracking System (CETS). The CETS program—already in use in several locations around the world—is designed to streamline investigations and integrate with other CETS operations so that law enforcement agencies can enhance their cooperation and efficiently move their cases forward.

"CETS has tremendous potential for the FBI," said Special Agent Barbara Cordero, a veteran cyber investigator who manages research, development, and training for the Innocent Images National Initiative. "Eventually, when everyone is plugged into CETS, it will allow law enforcement everywhere to share key information."

"If I'm in a small police department in Iowa, I might not know that another department in Maryland is investigating the same subject I am investigating," Cordero explained. "CETS will tell me that, along with other important information."

**Essentially, CETS is a repository that can be filled with records pertaining to child pornography and child exploitation cases.** The system can contain images, case information, identities of known offenders along with information about their Internet addresses, and other related material. The program can analyze millions of pornographic images, helping law enforcement personnel avoid duplication of effort. The program can also perform in-depth analyses, establishing links in cases that investigators might not have seen by themselves.

"CETS has the ability to put the same information in one place and make it available in a unified standard for everyone," said Special Agent Charles Wilder, who heads DARC. "That's important because the Internet has removed all geographic boundaries in these types of crimes."

The CETS program was created by Microsoft at the request of the Royal Canadian Mounted Police National Child Exploitation Coordination Center—investigators there wanted a system designed specifically for child exploitation cases. The program is now being used in Canada and Australia—and Interpol, the international police organization, is working with several of its member countries to integrate CETS into its existing systems.

The ultimate goal is to expand the number of CETS users and to one day integrate all the operations so investigators can share information in a truly global way. "Right now," Cordero said, "the immediate benefit for the FBI is that CETS saves us a tremendous amount of time in the image review process. Bad guys who trade pornographic images have massive collections," she said. "We regularly seize hundreds of thousands of images. CETS makes the review process extremely efficient."

She added, "The FBI has terrific partnerships with cyber investigators in the U.S. and around the world. As we move forward, CETS will allow us to strengthen those partnerships by sharing more and more critical information. This type of technology is a model for the future."

Left: Special Agent Arthur Thurston, head of the FBI's London office during World War II

# A Byte Out of History

## A Most Helpful Ostrich: Using Ultra Intelligence in World War II

Winston Churchill and Dwight Eisenhower thought the intelligence was vital to Allied victory in World War II. Eisenhower is said to have called it "decisive." Churchill was reported to be even stronger in his assessment to King George VI.

The intelligence was called "Ultra"—because it was so highly secret—and it consisted of intercepted and later decoded radio and cable messages sent by the Nazis to their clandestine networks in Europe and South America during the war. Ultra was launched by British intelligence in 1941 and ultimately became a cooperative Allied effort.

**The FBI learned of Ultra in November 1942 and was immediately interested because of its implications on investigative efforts during the war.** We gave the intelligence we were able to obtain through Ultra another name—"Ostrich." The code name was arbitrary, but the information it provided was anything but. The intercepted messages—whether decrypted by British cipher experts, U.S. Army and Navy code breakers, or the new and rapidly improving cryptanalysis team in the FBI Laboratory—were invaluable to our work to protect the homeland from German espionage and sabotage.

The Ostrich information was often hard to come by. In those days, secrecy was paramount and cooperation was just beginning between the FBI and overseas intelligence services like the British Secret Intelligence Service, now more commonly known as MI-6. But through the Bureau's newly formed legal attaché office in London—headed by Special Agent Arthur Thurston and his assistant, John Cimperman—the FBI began reviewing the British decrypts at MI-6 in January 1943. The bits of intelligence related to possible German espionage on U.S. soil were passed to FBI Headquarters and then on to Bureau agents for action.

**The information was especially valuable to our work in South America, where in June 1940—under orders from President Franklin D. Roosevelt—the FBI had set up the Special Intelligence Service, or SIS, to pinpoint and neutralize Nazi spy rings and intelligence activities in the Western Hemisphere.**

It helped us, for example, in Argentina, where a network of secret Nazi radio stations had sprung up after being shut down in Brazil in 1942. With the help of Ostrich messages decoded both by the British and by cryptanalysts in the FBI Laboratory, the Bureau learned of the strong political influence and extensive intelligence activities of German agent Johannes Becker, mapped out the operation of his ring, disrupted its work throughout the war, and later shut it down completely in the summer of 1945.

Without Ostrich, the FBI would not have been as successful in pinning down the extent of Nazi espionage in South America through the SIS. On a broader level, Ostrich intelligence enabled the Bureau to control the movements of its double agents and ensure they were successful in penetrating German intelligence. It was, in the end, one of the FBI's most significant sources of intelligence in World War II.

**Of course, as the war ended, so did the information stream provided by Ostrich and Ultra.** But the lessons learned would continue on—most especially in our efforts to penetrate Soviet intelligence in the coming Cold War through cooperative cryptanalytic ventures like Venona. Today, such pioneering information-sharing initiatives are now widespread and widely recognized as key to the work of the FBI and its global partners in protecting the world from terrorists, spies, and dangerous criminals.

# 18 Child Porn Websites Shut Down

## Result of Joint U.S.-China Cooperation

In another example of the increasingly international nature of crime, a man was recently indicted on federal charges of running 18 Chinese-language child pornography websites out of his apartment in Flushing, New York. The websites were being advertised to Chinese-speaking individuals in China, in the U.S., and other countries.

**This case serves as an example of something else as well:** the increasingly international nature of law enforcement. While the FBI investigated this case in the U.S., we received what U.S. Attorney Preet Bharara of the Southern District of New York called "extensive cooperation and assistance" from the Chinese Ministry of Public Security.

**How it all started.** In late 2010, the FBI—through our legal attaché office in Beijing—received information from Chinese officials about their investigation of a large-scale child pornography website housed on U.S. servers. And one of their main suspects, a Chinese-born man, was living in New York. So our New York office opened an investigation under our Innocent Images National Initiative and instituted an undercover operation.

**The investigation.** While the main webpage advertised the various categories of pornographic pictures that were available, our undercover agents—with the help of an FBI Chinese language specialist—discovered that in order to actually view, post, or download the pornography, you had to pay a membership fee ($25 quarterly, $50 annually, and $100 for a "lifetime" membership). The website conveniently accepted all payment types—credit cards, wire and bank transfers, online payments, and even cash that could be mailed to what turned out to be a money transfer office in New York. After becoming "members," the agents saw hundreds of disturbing pictures and videos of children of all different nationalities engaging in sexually explicit conduct.

Through our investigative efforts, we were able to determine that the site—and its related online payment system—resided on the servers of a web hosting company in Dallas and that the subscriber of the website domain lived in Flushing. We also traced two e-mail accounts—one featured on the site and the other affiliated with the

website domain—back to the same individual. Through billing information, we learned that the man had made about $20,000 per month from his subscribers. We believe he had been operating the site since at least 2007.

After the arrest, we identified 17 additional Chinese-language child pornography websites he allegedly maintained and operated. We also seized two servers in Dallas where those sites were hosted. All 18 websites have been shut down.

**During the course of the operation, FBI and Chinese investigators and prosecutors met to discuss the case and to talk about future cooperation on similar cases.**

One concrete outcome of this partnership? The Ministry of Public Security sent its first Chinese officer to join the FBI's Innocent Images International Task Force and receive specialized training on such topics as legal principles, emerging trends and technologies, and investigative techniques. Once the fall 2011 training session is completed, the task force will number 100 officers in 43 countries. Since its launch in 2004, the task force has built an international network of Internet child sexual exploitation investigators who share intelligence and work joint operations across national borders. Exactly what's needed to combat the many child pornographers using the Internet to extend their nefarious reach around the globe.


Left: A latent print removed from the victim's car was determined to be a match to the suspect's fingerprint (inset) contained in IAFIS.

# Houston Cold Case Solved

## Forensics Personnel Honored by FBI

On December 14, 1969, a young single mother named Diane Maxwell Jackson arrived for her shift as a Southwestern Bell telephone operator in Houston. After parking her car in the company lot, she was forced into a nearby shack by an unknown individual and brutally raped, strangled, and stabbed to death. After a thorough investigation by the Houston Police Department (PD), no suspects were identified, and the latent prints lifted from the outside of the victim's car were filed away.

**Decades later, assisted by advances in technology and interest from the victim's brother, the case was reopened and ultimately solved.** And most recently, the Houston PD detective and Texas Department of Public Safety latent print technician so instrumental in the outcome were honored by the FBI with the 2011 "Latent Hit of the Year" Award.

This award is given out annually for a latent print identification made after a search of our Integrated Automated Fingerprint Identification System (IAFIS) that results in a conviction for a major violent crime. IAFIS is a national fingerprint and criminal history system that responds to requests from our partners and our own investigators to help solve and prevent crimes and terrorism. It currently houses the fingerprints of more than 70 million criminal subjects.

**Houston case background:** Years passed after Jackson's murder, and with no new leads, the case went cold. But in 1989, David Maxwell, the victim's brother, began reviewing the file on his sister's death. Maxwell reconsidered his plan to become a lawyer after his sister died and instead joined the Texas State Highway Patrol and later the Texas Rangers. He asked the Houston PD to review the original evidence and witness reports for any new leads.
A Houston newspaper ran an article publicizing the murder and requesting assistance from the public. At the same time, the Houston PD began a search for the latent prints lifted from the victim's car.

Once located, the prints were searched against the Houston PD's local fingerprint database and the Texas Department of Public Safety's Automated Fingerprint Identification System. Neither searched yielded a positive ID.

On July 23, 2003, Texas Department of Public Safety Latent Print Technician Jill Kinkade prepared the prints for a search of the FBI's IAFIS. In less than five hours, the system returned a response containing 20 potential matches, and Kinkade determined that the latent print evidence was a match to the number one candidate—James Ray Davis.

**Honing in on a suspect.** Investigators discovered that Davis had been arrested for various crimes before and after Diane Maxwell Jackson's murder—in fact, he had just finished a prison term nine days before the murder.

Learning about the latent print identification of Davis, Houston PD Sergeant James Ramsey—the case's lead investigator—quickly located the suspect living along the Texas-Arkansas border. Investigators knew that because his fingerprints were recovered from the outside of the victim's car, they would likely need a confession in order to get a conviction, After being presented with the forensic evidence and photographs of the crime scene, Davis admitted to the crimes.

He pled guilty in court, and on November 24, 2003, 34 years after the homicide, James Ray Davis was sentenced to life in prison for the rape and murder of Diane Maxwell Jackson.

# The FBI Since 9/11

## D.C. Museum Updates Popular Exhibit

The FBI's fight against terrorism—our top priority since 9/11—is the subject of a new addition to a popular museum exhibit in the nation's capital.

**"War on Terror: The FBI's New Focus," opened last month at the Newseum, a museum devoted to the news and journalism.** The new installment, part of the larger exhibit "G-Men and Journalists: Top News Stories of the FBI's First Century," contains 60 artifacts from the 9/11 investigation and other well-known terror plots.

"G-Men and Journalists," which opened in 2008 and has drawn more than two million visitors, "has been one of our most popular exhibits," said Cathy Trost, the Newseum's director of exhibit development. "But we realized we also needed to tell the story of the Bureau's fight against terrorism, which has really defined the modern FBI."

Some of the artifacts on display are small and deeply personal, such as the pocketbook of Ruth McCourt, which contained credit cards and a snapshot of Ruth and her 4-year-old daughter, who were on their way to Disneyland when their plane—Flight 175—hit the World Trade Center on 9/11. Our Evidence Response Teams recovered thousands of these types of personal items, and our Office for Victim Assistance later returned many of them to family members.

Also on display is a collection of damaged cell phones and pagers recovered from the World Trade Center rubble. For days after the attack, as first responders and law enforcement teams searched for survivors and evidence, these buried devices rang and rang as victims' families and loved ones desperately tried to make a connection.

**Other artifacts are large, chilling reminders of the 9/11 attack's deadly destruction, including two pieces of the airplane engines—one weighing some 1,500 pounds—that crashed into the World Trade Center towers and were recovered blocks from Ground Zero.**

The exhibit also features other investigations besides the 9/11 attack, including the case of shoe bomber Richard Reid. Trained by al Qaeda, Reid tried to blow up a flight from Paris to Miami in December 2001 using explosives hidden in his hiking boots. The actual shoes are on display—along with a collection of belts used by passengers to subdue him until the flight landed and he was taken into custody.


**Some of the artifacts on display in the "War on Terror: The FBI's New Focus" exhibit. Photo courtesy of the Newseum.**

"People are moved by the power of these artifacts," Trost said.

The "War on Terror" exhibit, like "G-Men and Journalists," was the result of a collaboration between the Newseum and the FBI—just one of the many ways our Office of Public Affairs tries to inform the public about the Bureau, its history, its people, and its mission.

"The ability to see these real pieces of history from some of our most important cases helps the public understand the Bureau's mission and how critical it is to the nation's security," said Mike Kortan, FBI assistant director of public affairs. Kortan noted that the FBI is also featured at the National Museum of Crime & Punishment and the International Spy Museum and will be represented at the National Law Enforcement Museum—all located near FBI Headquarters in Washington. The Bureau is also working with the Ground Zero Museum in New York, he said.


Left: Vahid Majidi, assistant director of the FBI's Weapons of Mass Destruction Directorate, discusses changes the Bureau has made since a bio-terrorism attack in 2001.

# The FBI Since 9/11

## Exec Discusses Improvements Since Anthrax Attacks

In the decade since deadly anthrax spores were sent through the mail in 2001, killing five people and sickening 22 others, the FBI has made significant advances in efforts to prevent and identify bio-terror threats. That was the message delivered Tuesday at a Senate hearing entitled: "Ten Years After 9/11 and the Anthrax Attacks: Protecting Against Biological Threats."

On a panel of federal experts that included the Departments of Homeland Security and Health and Human Services, Vahid Majidi—head of the FBI's Weapons of Mass Destruction Directorate—described how much the Bureau has changed since the first of several anthrax-laced letters began arriving in mailboxes a week after 9/11. Our primary focus is on prevention.

**"Domestic and international terrorist groups, such as al Qaeda and its affiliates, have shown unwavering interest in using biological agents and toxins,"** Majidi said during the hearing before the Committee on Homeland Security and Governmental Affairs. "The FBI is dedicated to protecting our nation and will continue to collaborate with the scientific community to proactively address new biological threats on the horizon."

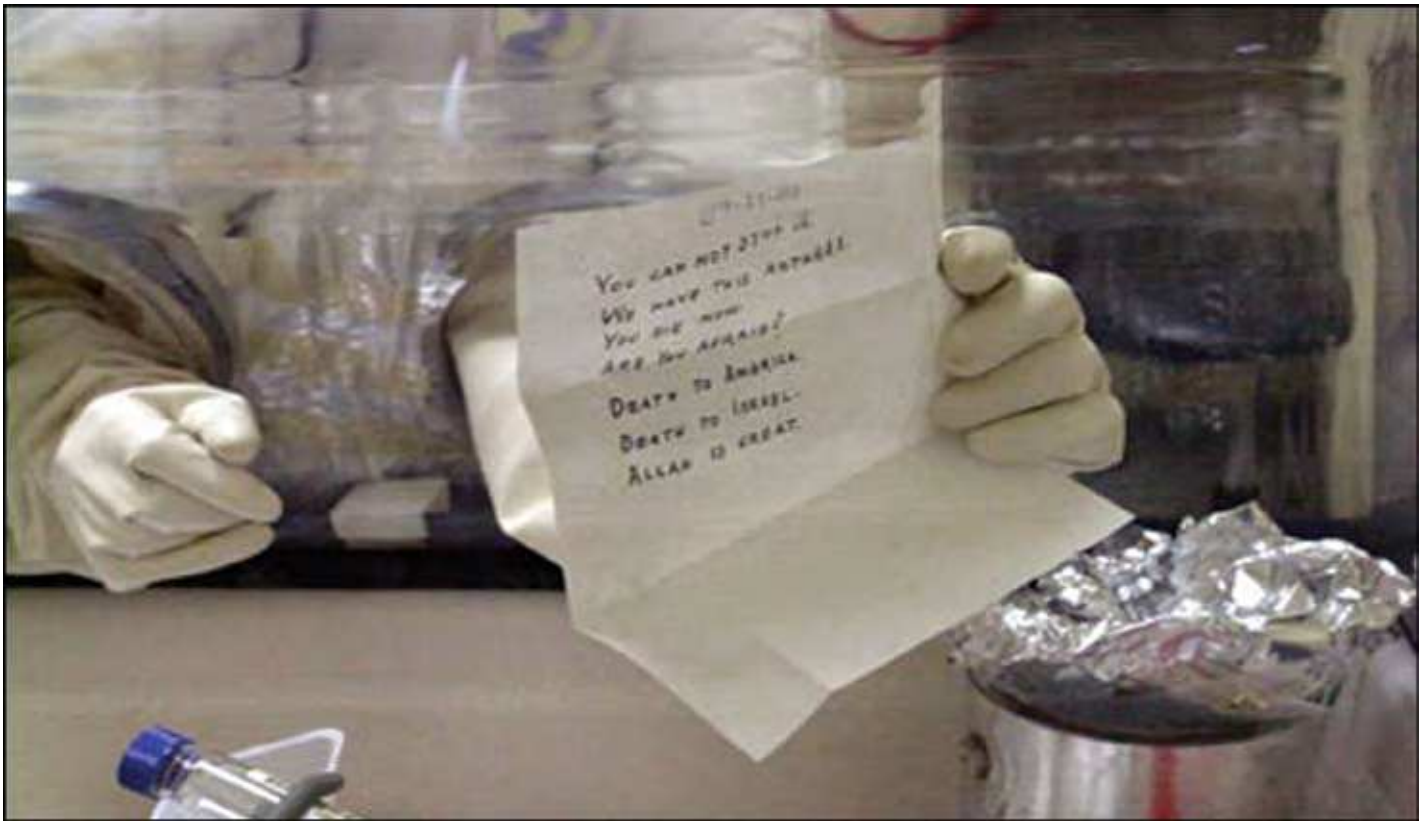
In response to the anthrax mailings, the FBI retooled to better target the bio-terror threat and to nurture relationships with like-minded partners in the scientific, health, agricultural, and law-enforcement communities.

In 2004, the 9/11 Commission recommended the FBI carve out a specialized branch of personnel to focus on counterintelligence and on counterterrorism—the Bureau's top priority. In 2005, FBI Director Robert S. Mueller assigned the newly formed National Security Branch to create an operational element to focus on chemical, biological, radiological, nuclear, and explosive matters—what in 2006 became the Weapons of Mass Destruction Directorate (WMDD). Over the last five years, Majidi said, the directorate has "developed and refined capabilities."

**"WMDD's primary mission is the prevention of WMD terrorism and proliferation through proactive programs," Majidi said.** While specific methodologies remain classified, Majidi listed a number of programs and initiatives the FBI created or collaborates on to identify, thwart, and investigate threats.

- All 56 field offices have a Weapons of Mass Destruction coordinator who fosters local relationships with labs, biological companies, and academia and coordinates with partner agencies in the event of a crisis response.
- The FBI and the Centers for Disease Control and Prevention developed the Joint Criminal and Epidemiological Investigations training program to improve efforts to identify threats that are intentional or naturally occurring.
- WMDD developed the Biological Sciences and Academic Workshop initiatives to build partnerships with academic communities and identify vulnerabilities, such attempts by terrorist groups to exploit experts with access to biological agents.
- The FBI Laboratory developed and implemented the Hazardous Evidence Analysis Team, or HEAT program, that provides advanced training for forensic examiners to allow them to collect evidence in high-containment labs.

"The FBI addresses bioterrorism threats by identifying points of vulnerability for biological agents, acquisitions, weapons development, and, ultimately, the execution phase," Majidi told the panel. To that end, his prepared remarks outlined a few of the hundreds of cases of biological substances or suspicious powders the FBI has probed since 2006. They include a Pennsylvania man who was infected by naturally occurring anthrax in 2006 and a




**Amerithrax Investigation**

Soon after the terrorist attacks of 9/11, letters laced with anthrax began appearing in the U.S. mail. Five Americans were killed and 17 were sickened in what became the worst biological attacks in U.S. history.

The ensuing investigation by the FBI and its partners—code-named "Amerithrax"—has been one of the largest and most complex in the history of law enforcement.

In August 2008, Department of Justice and FBI officials announced a breakthrough in the case and released documents and information showing that charges were about to be brought against Dr. Bruce Ivins, who took his own life before those charges could be filed. On February 19, 2010, the Justice Department, the FBI, and the U.S. Postal Inspection Service formally concluded the investigation into the 2001 anthrax attacks and issued an Investigative Summary.

The Amerithrax Task Force—which consisted of roughly 25 to 30 full-time investigators from the FBI, the U.S. Postal Inspection Service, and other law enforcement agencies, as well as federal prosecutors from the District of Columbia and the Justice Department's Counterterrorism Section—expended hundreds of thousands of investigator work hours on this case. Their efforts involved more than 10,000 witness interviews on six different continents, the execution of 80 searches, and the recovery of more than 6,000 items of potential evidence during the course of the investigation. The case involved the issuance of more than 5,750 grand jury subpoenas and the collection of 5,730 environmental samples from 60 site locations. In addition, new scientific methods were developed that ultimately led to the break in the case—methods that could have a far-reaching impact on future investigations.

Las Vegas man who was cooking up the pathogen ricin in his hotel room in 2008.

"Significant progress and partnerships have been made with all levels of government, industry, and the scientific community since the creation of the WMDD," Majidi said, "all of which improve the FBI's capabilities in its mission."


Left: Law enforcement officers in 22 states and Puerto Rico were feloniously killed in 2010.

# In the Line of Duty

## 56 Officers Feloniously Killed in 2010

Fifty-six law enforcement officers in 22 states and Puerto Rico were feloniously killed in 2010, and more than 53,000 officers were assaulted during the same period, according to statistics released by the FBI.

The annual *Law Enforcement Officers Killed and Assaulted* report released today offers the most complete public picture of the fatal circumstances that officers faced in 2010. In chilling detail, the report summarizes most of last year's fatal confrontations and illustrates a reality that every officer continually trains to recognize: that there are no routine engagements. Among the scenarios:

- Two West Memphis Police Department officers were killed during a traffic stop when a 16-year-old passenger exited the vehicle and opened fire with a semiautomatic rifle.
- A Chicago Police Department officer at the end of his shift was removing his gear near his car in the department's parking lot when a man ambushed the 43-year-old officer and shot him with his own weapon.
- A 62-year-old deputy sheriff in Mississippi was shot and killed by an uncooperative suspect while responding to a domestic disturbance call.

Information in the report, which is collected each year through the FBI's Uniform Crime Reporting (UCR) Program, is intended to provide law enforcement agencies with detailed descriptions of the circumstances leading up to officer fatalities. The data can then be incorporated into tactical training.

"Only when detectives, use-of-force investigators, supervisors, and administrators examine the various components of the deadly mix will a greater understanding of these encounters emerge," FBI researchers wrote in a study called Violent Encounters, an in-depth look at years of fatal altercations like those in today's report. "To make an objective assessment of each case, it is necessary to carefully and completely examine all aspects of the incident thus allowing the facts to surface."

The 56 officers killed is an increase over 2009, when 48 officers were killed. However, significant conclusions may not be drawn from year-to-year comparisons given the nature of the statistics. Ten years ago, for example, 70 officers were killed in the line of duty (excluding the events of 9/11), and five years ago 48 officers were feloniously killed.

The 2010 report also shows 72 officers were accidently killed in the line of duty, almost all of them involving vehicles. Meanwhile, 53,469 officers were assaulted while on duty—a figure that amounts to one in 10 of the sworn officers in more than 11,000 agencies that reported data.

All told, the figures illustrate the inherent dangers of law enforcement. Here's a look at some of the data contained in the report:

- Offenders used firearms to kill all but one of the 56 victim officers; one officer was killed by a vehicle used as a weapon.
- Of the 56 officers feloniously killed, 15 were ambushed, 14 were in arrest situations, seven were performing traffic stops, and six were answering disturbance calls.
- One in three officer assaults occurred while responding to disturbance calls; 14.7 percent occurred while officers were attempting arrests.
- The average age of officers killed feloniously and accidentally was, respectively, 38 and 39.

The UCR Program, part of the FBI's Criminal Justice Information Services Division, has been collecting and publishing law enforcement statistics since 1937, most notably the annual *Crime in the United States* reports. In 1972, the FBI began producing detailed reports on officer fatalities after the larger law enforcement community sought the Bureau's involvement in preventing and investigating officer deaths.

# Operation Ghost Stories

## Inside the Russian Spy Case

The arrests of 10 Russian spies last year provided a chilling reminder that espionage on U.S. soil did not disappear when the Cold War ended. The highly publicized case also offered a rare glimpse into the sensitive world of counterintelligence and the FBI's efforts to safeguard the nation from those who would steal our vital secrets.

**Our case against the Russian Foreign Intelligence Service (SVR) operatives—dubbed Operation Ghost Stories—went on for more than a decade.** Today we are releasing dozens of still images, surveillance video clips, and documents related to the investigation as part of a Freedom of Information Act request.

Although the SVR "illegals," as they were called, never got their hands on any classified documents, their intent from the start was serious, well-funded by the SVR, and far-ranging.

"The Russian government spent significant funds and many years training and deploying these operatives," said one of our counterintelligence agents who worked on the case. "No government does that without expecting a return on its investment."

Our agents and analysts watched the deep-cover operatives as they established themselves in the U.S. (some by using stolen identities) and went about leading seemingly normal lives—getting married, buying homes, raising children, and assimilating into American society.

Using surveillance and sophisticated techniques, aided by support from intelligence analysts, investigators gathered information to understand the threat posed by the spies as well as their methods, or tradecraft.

**The SVR was in it for the long haul. The illegals were content to wait decades to obtain their objective, which was to develop sources of information in U.S. policymaking circles.**

Although they didn't achieve that objective, the agent said, "without us there to stop them, given enough time they would have eventually become successful."

After years of gathering intelligence and making sure we knew who all the players were, we arrested the illegals on June 27, 2010. Weeks later, they pled guilty in federal court to conspiring to serve as unlawful agents of the Russian Federation within the U.S.

Russian spy Christopher Metsos, right, swaps information in a "brush pass" with an official from the Russian Mission in New York in 2004. The image from a video is part of a trove of documents, photos, and surveillance released by the FBI as part of a Freedom of Information Act request.

**The plea represented the culmination of a remarkable effort on the part of countless Bureau personnel, including agents, analysts, surveillance teams, linguists, and others.**

"Operation Ghost Stories sends a message to foreign intelligence services that espionage threats to the U.S. will not be tolerated," our agent said. "The FBI's counterintelligence mission is to identify, disrupt, and defeat the activities of foreign espionage agents, and we take that job very seriously."

Usually, the critical work of our Counterintelligence Division is carried out in conjunction with our partners in the U.S. intelligence community with the utmost secrecy. Because the public rarely hears about those efforts, it would be easy to forget how real the threat of espionage is.

"And the threat is not limited to the Russians," the agent said. "There are a lot of foreign services who want what we have, and that's why we have agents and analysts in FBI field offices across the country working with other intelligence community partners every day to address these threats."

Left: Surveillance photo of two subjects of Operation Ghost Stories, an investigation into a Russian spy ring operating in the U.S.

# FBI Counterintelligence National Strategy

## A Blueprint for Protecting U.S. Secrets

Espionage may seem like a throwback to earlier days of world wars and cold wars, but the threat is real and as serious as ever.

**We see it—and work hard to counter it—all the time.** It's not just the more traditional spies passing U.S. secrets to foreign governments, either to fatten their own wallets or to advance their ideological agendas. It's also students and scientists and plenty of others stealing the valuable trade secrets of American universities and businesses—the ingenuity that drives our economy—and providing them to other countries. It's nefarious actors sending controlled technologies overseas that help build bombs and weapons of mass destruction designed to hurt and kill Americans and others.

In late October, in fact, we took part in a multi-agency and multi-national operation that led to the indictment of five citizens of Singapore and four of their companies for illegally exporting thousands of radio frequency modules from the U.S. Allegedly, at least 16 modules were later found in unexploded improvised explosive devices in Iraq.

As the lead agency for exposing, preventing, and investigating intelligence activities on U.S. soil, the FBI continues to work to combat these threats using our full suite of investigative and intelligence capabilities. We've mapped out our blueprint in what we call our **Counterintelligence National Strategy**, which is regularly updated to focus resources on the most serious current and emerging threats.

The strategy itself is classified, but we can tell you what its overall goals are:

- **Keep weapons of mass destruction, advanced conventional weapons, and related technology from falling into the wrong hands**—using intelligence to drive our investigative efforts to keep threats from becoming reality. Our new Counterproliferation Center will play a major role here.
- **Protect the secrets of the U.S. intelligence community**—again, using intelligence to focus investigations and collaborating with government partners to reduce the risk of espionage and insider threats.
- **Protect the nation's critical assets**—like our advanced technologies and sensitive information in the defense, intelligence, economic, financial, public health, and science and technology sectors.
- **Counter the activities of foreign spies**—whether they are representatives of foreign intelligence agencies or governments or are acting on their behalf, they all want the same thing: to steal U.S. secrets. Through proactive investigations, we identify who they are and stop what they're doing.

**One important aspect of our counterintelligence strategy involves strategic partnerships.** And on that front, we focus on three specific areas:

- The sharing of expertise and resources of the FBI, the U.S. intelligence community, other U.S. government agencies, and global partners to combat foreign intelligence activities;
- Coordination of U.S. intelligence community efforts to combat insider threats among its own ranks; and
- Partnerships with businesses and colleges and universities to strengthen information sharing and counterintelligence awareness.

**Focus on cyber activities.** Another key element of our counterintelligence strategy, according to FBI Counterintelligence Assistant Director Frank Figliuzzi, is its emphasis on detecting and deterring foreign-sponsored cyber intelligence threats to government and private sector information systems. "Sometimes," he said, "the bad guys don't have to physically be in the U.S. to steal targeted information…sometimes they can be halfway around the world, sitting at a keyboard."

# Phony Document Rings Broken Up

## Alleged California Ringleader Arrested

It just got a little harder to get a phony driver's license or Social Security card in the U.S.

**On November 3, more than 300 law enforcement officers from a variety of federal and local agencies executed dozens of search warrants and arrests involving fraudulent document rings operating in California, Illinois, and Texas that reached into a number of other states and Mexico.**

One of the main targets of the investigation was Alejandro Morales Serrano, who is believed to be a key player in this criminal conspiracy. Serrano and a number of his associates allegedly manufactured and sold the raw materials used to create the phony documents—like sheets of plastic laminates, monochrome card printer ribbons, hard plastic cards, and magnetic card reader/writer machines. Serrano was also one of those arrested during the law enforcement sweep.

The indictment alleges that the false documents were created on a large scale in California, Nevada, Oregon, Texas, Illinois, and Michigan. In addition to U.S. driver's licenses and Social Security cards, these documents also included U.S. Permanent Residency cards (a.k.a., "green cards"), Mexican consular ID cards, and Mexican driver's licenses.

**According to the indictment, the illegal document-making operation supported the manufacturing of fake driver's licenses for approximately 40 U.S. states and a number of Mexican states.**

Searches conducted during the takedown resulted in significant seizures from various residences, other locations, and vehicles and included plastic laminates used to produce the documents, computers, and stacks of phony documents that would have undoubtedly ended up on the black market had it not been for law enforcement's intervention.

The indictment doesn't specify when Serrano began his alleged "manufacturing" career, but it does state that he was heard on a law enforcement wiretap telling someone he'd been engaged in the business for more than a decade.


**What were the phony identification documents used for?** The investigation revealed that they were used by illegal aliens to get jobs as well as to apply for citizenship and residency-related benefits. We also believe that the operation supported other crimes—and criminals—like credit and bank fraud, tax fraud, identity theft, and pharmaceutical diversion.

Of course, one of law enforcement's concerns about fraudulent document activity is that a fake identity document could potentially end up in the hands of someone with a more nefarious plan in mind—like a spy or a terrorist trying to enter the U.S. to steal information or harm Americans.

Explained Steven Gomez, Special Agent in Charge of the Counterterrorism Branch in our Los Angeles office, "False documents are utilized by a wide variety of criminals to facilitate their illegal activity as well as to conceal their identities from law enforcement. This multi-agency operation disrupted criminal activity, but also identified a national security vulnerability."

**In a related case worked by the FBI and the Los Angeles Sheriff's Department, several individuals were identified in a conspiracy to manufacture and distribute false identification documents with the materials supplied by Serrano.**

Both investigations and subsequent takedowns were the result of the collaborative efforts of many agencies, including the FBI, the Los Angeles Police Department, the Los Angeles County Sheriff's Department, the Drug Enforcement Administration, the U.S. Immigration and Customers Enforcement, as well as agencies in Illinois, Texas, and elsewhere in California.


# Operation Ghost Click

## International Cyber Ring That Infected Millions of Computers Dismantled

Six Estonian nationals have been arrested and charged with running a sophisticated Internet fraud ring that infected millions of computers worldwide with a virus and enabled the thieves to manipulate the multi-billion-dollar Internet advertising industry. Users of infected machines were unaware that their computers had been compromised—or that the malicious software rendered their machines vulnerable to a host of other viruses.

**Details of the two-year FBI investigation called Operation Ghost Click were announced today in New York when a federal indictment was unsealed.** Officials also described their efforts to make sure infected users' Internet access would not be disrupted as a result of the operation.

The indictment, said Janice Fedarcyk, assistant director in charge of our New York office, "describes an intricate international conspiracy conceived and carried out by sophisticated criminals." She added, "The harm inflicted by the defendants was not merely a matter of reaping illegitimate income."

Beginning in 2007, the cyber ring used a class of malware called DNSChanger to infect approximately 4 million computers in more than 100 countries. There were about 500,000 infections in the U.S., including computers belonging to individuals, businesses, and government agencies such as NASA. The thieves were able to manipulate Internet advertising to generate at least $14 million in illicit fees. In some cases, the malware had the additional effect of preventing users' anti-virus software and operating systems from updating, thereby exposing infected machines to even more malicious software.

"They were organized and operating as a traditional business but profiting illegally as the result of the malware," said one of our cyber agents who worked the case. "There was a level of complexity here that we haven't seen before."

DNS—Domain Name System—is a critical Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse websites or send e-mail.

**DNSChanger redirected unsuspecting users to rogue servers controlled by the cyber thieves, allowing them to manipulate users' web activity.** When users of infected computers clicked on the link for the official website of iTunes, for example, they were instead taken to a website for a business unaffiliated with Apple Inc. that purported to sell Apple software. Not only did the cyber thieves make money from these schemes, they deprived legitimate website operators and advertisers of substantial revenue.

The six cyber criminals were taken into custody yesterday in Estonia by local authorities, and the U.S. will seek to extradite them. In conjunction with the arrests, U.S. authorities seized computers and rogue DNS servers at various locations. As part of a federal court order, the rogue DNS servers have been replaced with legitimate servers in the hopes that users who were infected will not have their Internet access disrupted.

It is important to note that the replacement servers will not remove the DNSChanger malware—or other viruses it may have facilitated—from infected computers. Users who believe their computers may be infected should contact a computer professional. They can also find additional information in the links on the FBI website, including how to register as a victim of the DNSChanger malware. And the FBI's Office for Victim Assistance will provide case updates periodically at 877-236-8947.

# Hate Crimes Remain Steady

## 2010 FBI Report Released

Intimidation…vandalism…assault…rape…murder. These are crimes by anyone's definition. But add an element of bias against the victims—because of their race or religion, for example—and these traditional crimes become hate crimes.

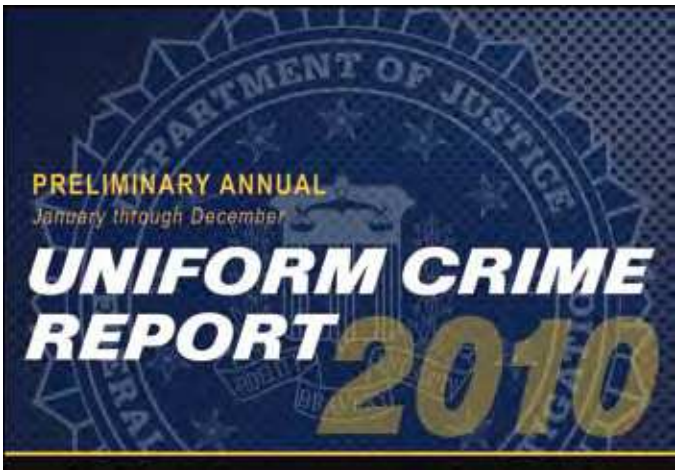
And based on data from the FBI's Hate Crime Statistics report for 2010, the 6,628 hate crime incidents reported to us by our law enforcement partners stayed consistent with the 6,604 incidents reported in 2009.

**Today, we're releasing on our website the full 2010 report, which contains information about the types of biases that motivate hate crimes, the nature of the offenses, and some information about the victims and offenders.** It also breaks down hate crimes by jurisdiction and includes data by state and by agency.

The hate crimes report is fairly reflective of the country—agencies that participated in the Uniform Crime Reporting Hate Crime Statistics Program effort in 2010 represented more than 285 million people, or 92.3 percent of the nation's population, and their jurisdictions covered 49 states and the District of Columbia. Of the 14,977 agencies that submitted data, 1,949 reported that hate crime incidents had occurred in their jurisdictions.

**Here are some of the report's highlights:**

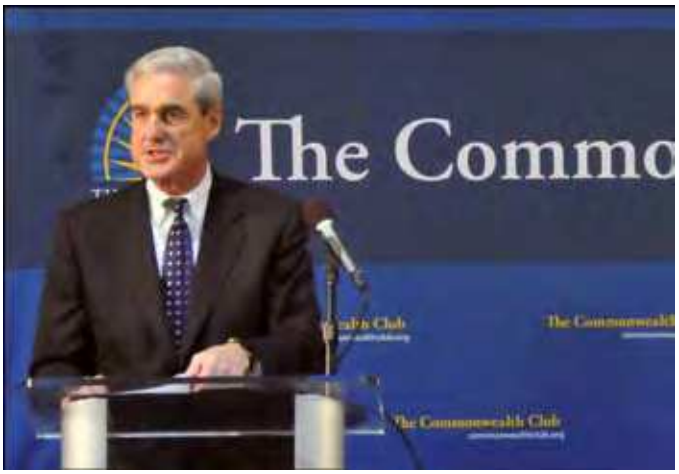
- Law enforcement reported 8,208 victims of hate crimes—a "victim" can be an individual, a business, an institution, or society as a whole.
- Of the 6,628 hate crime incidents reported to us for 2010, nearly all (6,624) involved a single bias—47.3 percent of the single-bias incidents were motivated by race; 20 percent by religion; 19.3 by sexual orientation; 12.8 percent by an ethnicity/national origin bias; and 0.6 by physical or mental disability.
- As a result of the 2009 Matthew Shepard and James Byrd, Jr., Hate Crime Prevention Act, the FBI is implementing changes to collect additional data for crimes motivated by a bias against a particular gender or gender identity, as well as for hate crimes committed by or directed against juveniles.
- A reported 4,824 offenses were crimes against persons—intimidation accounted for 46.2 percent of these offenses; simple assault for 34.8 percent; and aggravated assault for 18.4 percent.




- There were 2,861 reported offenses of crimes against property—the majority (81.1 percent) were acts of destruction/damage/vandalism.
- Of the 6,008 known offenders, 58.6 were white and 18.4 percent were black.
- 31.4 percent of reported hate crime incidents took place in or near homes.

**The FBI takes its role in investigating hate crimes very seriously—it's the number one priority of our civil rights program.** "Almost a fourth of our 2010 civil rights caseload involved crimes motivated by a particular bias against the victim," said Eric Thomas, our civil rights chief in Washington, D.C., "and we frequently worked these cases with state and local law enforcement to ensure that justice was done—whether at the state level or at the federal level."

This report, and the FBI's hate crime data collection effort as a whole, would not have been possible without the support of national and state criminal justice organizations and the thousands of law enforcement agencies nationwide whose officers investigate, identify, and report hate crimes to us.




Left: Director Robert S. Mueller delivers remarks in San Francisco. "Terrorists, spies, and hackers are always thinking of new ways to harm us," Mueller said.

# Terrorists, Spies, and Hackers

## The New National Security Landscape

Cyber thieves in Eastern Europe drain bank accounts in America. Spies steal industry secrets and sell them overseas. And alone in their bedrooms, disaffected youths become radicalized by Internet propaganda and vow to wage jihad.

**It is difficult to remember a time when Americans did not have to worry about terrorists plotting violence on U.S. soil and criminals reaching through the Internet to target individuals, businesses, and government, but that is how drastically the world has changed since the 9/11 attacks.**

"The horrific events of that day were the prelude to a decade of political, economic, and cultural transformation," said FBI Director Robert S. Mueller, "and globalization and technology have accelerated these changes."

The hyper-connectivity that helped spawn this new globalization is empowering "both friend and foe alike," Mueller said this afternoon during a speech in San Francisco. "Today, our world can change in the blink of an eye. … If we in the FBI fail to recognize how the world is changing, the consequences can be devastating."

Mueller noted that "terrorists, spies, and hackers are always thinking of new ways to harm us." He provided examples of several recent cases and outlined how the Bureau plans to stay ahead of these threats while remaining ever-mindful of protecting civil liberties.

Regarding terrorism, al Qaeda has been weakened since 9/11, and dozens of attacks have been prevented. But "core al Qaeda operating out of Pakistan remains committed to high-profile attacks against the West," Mueller said—a fact confirmed by records seized from Usama Bin Laden's compound after his death. In Yemen, al Qaeda in the Arabian Peninsula has attempted several attacks on the U.S., Mueller added. And of particular concern are homegrown terrorists who may become self-radicalized online and are willing to act alone, which makes them difficult to find and to stop.

**In the area of espionage, "nations will always try to learn one another's secrets to gain political, military, or economic advantage," Mueller said. And because "so much sensitive data is now stored on computer networks," he added, "our adversaries often find it as effective, or even more effective, to steal secrets through cyber intrusions."**

And while state-sponsored cyber espionage is a growing problem, "it is but one aspect of the cyber threat," Mueller pointed out. Hacktivist groups, for example, are engaging in digital anarchy, and cyber attacks against our critical infrastructure are a real possibility.

The FBI must stay one step ahead of these threats by gathering and sharing intelligence and continuing to emphasize our partnerships. "No single agency, company, or nation can defeat these complex, global threats alone," Mueller said.

He also noted that the FBI needs the right tools to address evolving cyber threats, especially with regard to lawfully intercepting electronic communications from social networks. "Laws covering this area have not been updated since 1994—a lifetime ago in the Internet age," Mueller said. "So we are working with Congress, the courts, our law enforcement partners, and the private sector to ensure that our ability to intercept communications is not eroded by advances in technology."

While the Bureau must change to combat evolving threats, "our values can never change," Mueller said. "The rule of law will remain the FBI's guiding principle. In the end, we know we will be judged not only by our ability to keep Americans safe, but also by whether we safeguard the liberties for which we are fighting."

# Antitrust Enforcement

## Success of DOJ/FBI Partnership

What are the two greatest investments for most Americans? Homes and vehicles. And the FBI is working alongside our partners in the Antitrust Division at the Department of Justice (DOJ) to make sure consumers aren't defrauded by artificial increases in car prices or deflation of home values as a result of antitrust practices.

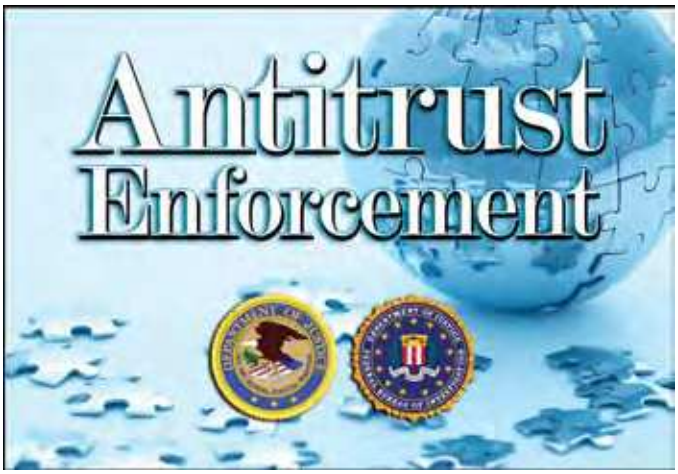
**For example:** In September, a Japanese auto parts company with operations in the U.S.—along with three of its executives—agreed to plead guilty in federal court in Detroit to a price-fixing and bid-rigging conspiracy with other companies involving the sale of parts to automobile manufacturers. The victims in this case? Other auto parts dealers who were shut out of the bidding process, car manufacturers who paid higher prices for auto parts, and ultimately, American car buyers who paid more for the price of a car.

**A second example:** As of October, 18 real estate investors have pled guilty in connection with two separate conspiracies to rig bids by agreeing to refrain from bidding against one another at public real estate foreclosure auctions in Northern California. When real estate properties are sold at these auctions, the proceeds pay off the mortgage and other debt attached to the property. These conspiracies cause the homes to be sold for less than they would go for at a fair and competitive auction. This lower price directly affects anyone in that neighborhood trying to sell their home.

Of course, antitrust violations go beyond auto parts and real estate. Recent criminal antitrust investigations have involved a number of industries, including freight-forwarding, concrete-mixing, optical disks, refrigerant compressors, and electronic LCD panels.

Antitrust activities raise prices and suppress competition, hurting businesses who play by the rules as well as consumers who pay more for products or services. And increasingly, profits from antitrust conspiracies to go foreign companies, which can impact the ability of U.S. businesses to remain competitive in the world market.

**DOJ's Antitrust Division is charged with civil and criminal enforcement of federal antitrust laws, and FBI investigators work jointly with DOJ antitrust prosecutors at several regional DOJ antitrust offices.** In the mid-1990s, that partnership really took off when we embarked on a highly aggressive antitrust enforcement




program, focusing resources on long-range investigations involving national and international conspiracies that greatly impacted U.S. commerce.

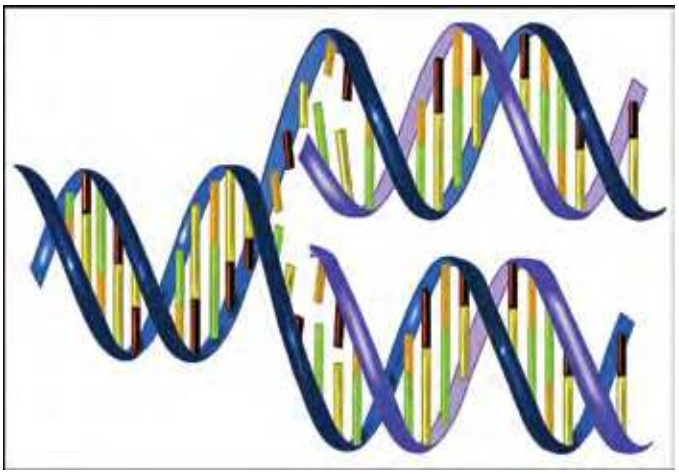
Antitrust violations include:

- Price-fixing—when competitors agree to raise, lower, or maintain the price at which their products or services are sold;
- Bid rigging—an agreement that competitors work out ahead of time about who's going to be awarded a contract and at what price; and
- Market allocation—involving agreements among conspirators on how to divvy up market share, either geographically or by customer.

To conduct antitrust investigations, we use the full arsenal of investigative tools available to us in all criminal cases, including the execution of search warrants on businesses, interviews, analysis of hard copy and electronic records, court-authorized electronic surveillance, and cooperating witnesses.

**Importance of international cooperation.** A vital piece of our antitrust effort is increased support and assistance from our global law enforcement partners—the Department of Justice currently has in place antitrust cooperation agreements with approximately 10 countries, including Russia and China.

These agreements come in very handy when our antitrust investigations lead us overseas…which happens nearly every day as more companies expand their operations worldwide.



# The FBI and DNA

## Part 1: A Look at the Nationwide System that Helps Solve Crimes

The use of DNA—which carries individuals' unique genetic information—to help solve crimes has become such a fundamental tool for law enforcement that it's hard to believe this technique of matching unknown profiles to known offenders is a fairly recent phenomenon.

The FBI launched the National DNA Index System (NDIS) in 1998—along with the Combined DNA Index System (CODIS) software to manage the program—and since that time it has become the world's largest repository of known offender DNA records. Last year, in partnership with local, state, and federal crime laboratories and law enforcement agencies, CODIS aided nearly 25,000 criminal investigations.

FBI.gov recently sat down with Douglas Hares, a Ph.D. scientist at the FBI Laboratory who is the custodian of the National DNA Database.

**Q: How did the Bureau come to play such a key role in using DNA to help solve crimes?**

**Hares:** DNA technology was first introduced in criminal court cases around 1988. When the FBI saw the potential for exchanging and comparing DNA profiles to help solve crimes—crimes that might not be solved in any other way—the concept of a national program was born. In 1994, Congress passed the DNA Identification Act, which gave the FBI authority to establish a national database. During the next few years, the FBI developed, tested, and implemented the CODIS software as well as training support for states authorized to collect DNA samples from offenders. In 1998, we started NDIS with nine participating states. Now, all 50 states participate, and NDIS currently contains over 10 million DNA profiles.

**Q: What is a DNA profile?**

**Hares:** A DNA profile, or type, is just a series of numbers. These numbers are assigned to an individual based on specific identification markers on his or her DNA molecule. In CODIS, those numbers represent a person's one-of-a-kind DNA profile.

**Q: How does CODIS use those profiles to solve crimes?**

**Hares:** A forensic laboratory receives evidence in a criminal investigation and is asked to perform DNA testing on that evidence. The evidence may be part of a rape case or a homicide. Or maybe there is a murder weapon that contains DNA. The DNA profile obtained from the crime scene evidence is called a forensic unknown. The laboratory doesn't know whose profile it is, but they know it is associated with the crime. The laboratory enters that profile into CODIS. If it's a local case, the profile is entered into the local CODIS system and uploaded to the state level. At the state level, the profile will be compared with all the offenders from that state's database. The forensic unknown may or may not match with other DNA records at the state level. On a weekly basis, the state uploads its DNA records to NDIS, the national level. We search the profile against all 50 states' offender profiles to see if there is a match; if there is, the CODIS software automatically returns messages in the system to the laboratories involved. The local labs evaluate the matches and release that information to the law enforcement agency. That is how a previously unknown DNA profile is associated with a known offender.

**Q: Who has access to CODIS?**

**Hares:** By federal law, access is generally limited to criminal justice agencies for law enforcement identification purposes. That federal law also authorizes access for criminal defense purposes to a defendant in connection with his or her case. CODIS was designed to ensure the confidentiality of the DNA record. No personal identifiers—such as name, Social Security number, or date of birth—are stored in CODIS.

# The FBI and DNA

## Part 2: More About the Nationwide System that Helps Solve Crimes

*Part 2 of an interview with Douglas Hares, a Ph.D. scientist at the FBI Laboratory who is the custodian of the National DNA Index System (NDIS), which is supported by the Combined DNA Index System (CODIS) software.*

**Q: How does CODIS handle high-profile cases such as serial killer Ted Bundy's DNA, which was recently tested so it could be entered into the system?**

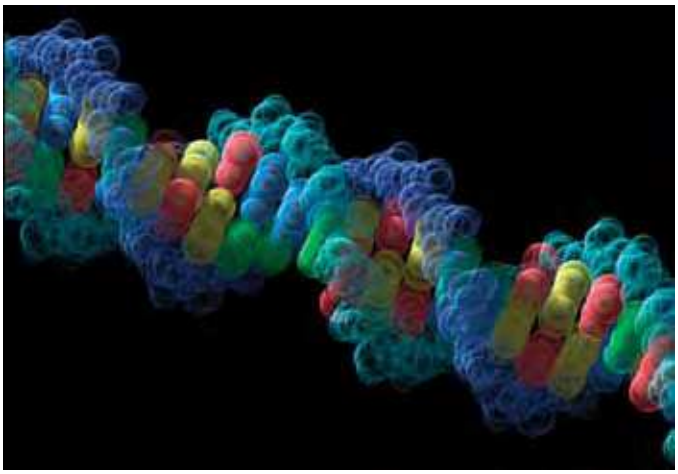
**Hares:** At the national level, we don't know about the evidentiary profiles entered into CODIS by the states. While the DNA profiles use specimen identification numbers, such identification numbers do not contain personal identifiers that would allow us to pick out a particular profile from the database as belonging to a specific person. For example, even if a state informs us that they have uploaded a high-profile sample like Bundy's, at the national level we don't know which profile is his because there is no personal identifying information attached to it. The system is designed to be completely anonymous to protect personal privacy—until a match occurs and the requesting state can learn the offender's identity. But this raises the importance of analyzing the DNA from such serial offenders, even if the offender is deceased, so that the DNA profile can be searched against those unsolved cold cases.

**Q: Is CODIS effective in cold cases?**

**Hares:** Absolutely—that demonstrates the power of CODIS. If you are able to obtain a DNA profile from a case that remained unsolved from years ago and place that profile into the system, there is a good chance you may get a hit because the offender may have committed other crimes and been required to provide a DNA sample.

**Q: How does technology help CODIS?**

**Hares:** It's important that all authorized profiles are entered into CODIS in a timely manner. The sooner profiles are entered into the system, the sooner CODIS can help solve crimes. Sometimes, when DNA database programs with limited resources expand to add categories of persons required to provide DNA samples, backlogs in samples to be analyzed and entered into CODIS may



develop. The FBI encountered such a situation when the law expanded DNA sample collection to federal arrestees and detainees. But thanks to a National Institute of Justice grant and the use of robotics and expert systems, we eliminated a backlog of more than 300,000 offender profiles in a matter of months. That achievement was recognized in a recent audit by the Department of Justice Office of Inspector General.

**Q: As technology is integrated into DNA processes, what can we expect from CODIS in the future?**

**Hares:** We have seen that as the number of DNA profiles in CODIS increases, the system helps solve more crimes. Now we are aiding more investigations in a single year than we did in the first five years of the system's existence. It's all due to the size of the database—increasing the number of authorized profiles for the state and national databases results in additional DNA profiles that could be linked to unsolved crimes. Since the creation of CODIS, we have aided over 152,000 investigations—that's an impressive number of crimes that may not have been solved by any other method. The statistics speak for themselves. As we continue to add more profiles, the potential to solve more crimes—and also to rule out suspects who are innocent—continues to increase.

Left: The FBI's Criminal Justice Information Services Division, or CJIS, is located in West Virginia.

# A Year of Records for CJIS

## Part 1: FBI's Largest Division Provides Information to Protect the Nation

The FBI's Criminal Justice Information Services Division—better known as CJIS—provides critical information to help our partners fight crime and protect the nation. Whether it's answering a patrolman's request for a subject's criminal record during a traffic stop, verifying that a potential gun buyer is not a felon, or ensuring that a local municipality is not hiring a teacher who is a registered sex offender, CJIS receives millions of electronic requests every day for criminal information records and returns responses with amazing speed and accuracy.

FBI.gov recently spoke with Special Agent David Cuthbertson, the newly appointed assistant director of CJIS, about the division's accomplishments in 2011 and what to expect from the FBI's largest division in the future.

**Q: CJIS has been described as a lifeline to law enforcement. What are some of the division's main programs?**

**Cuthbertson:** The term "lifeline" aptly describes what we do day in and day out at CJIS. Our main programs include NCIC—the National Crime Information Center—and the Interstate Identification Index, which is the nation's criminal history repository. NCIC is searched by law enforcement nearly 8 million times every day. And those requests—related to stolen property and information on wanted, missing, and unidentified persons—are returned to officers on the street within fractions of a second. NICS—the National Instant Criminal Background Check System—helps keep guns out of felons' hands. In the last fiscal year, NICS conducted more than 15.9 million background checks in accordance with federal law, and more than 76,000 gun transfers were denied based on buyers' criminal records. Our Law Enforcement National Data Exchange—N-DEx—provides a secure, online national information-sharing system for records related to bookings, arrests, probation, and parole report data. More than 4,100 agencies contribute to N-DEx, and the system has more than 124 million searchable records. And, of course, CJIS maintains the largest collection of fingerprint records in the world. During the last fiscal year, the Integrated Automated Fingerprint Identification System—IAFIS—identified more than 307,000 fugitives. These programs are only part of the important work we do at CJIS. Our recently released annual report highlights other programs and many of our record-setting accomplishments.

**Q: Does CJIS share information with partners outside of law enforcement?**

David Cuthbertson, assistant director of CJIS

**Cuthbertson:** Absolutely. We provide information to the U.S. intelligence community for national security matters, and our data is also relied upon for civil uses such as criminal checks for employment and licensing. Teachers and school bus drivers, for example, are subject to background checks as required by state law, and CJIS systems provide that information to authorized users.

**Q: Given the vast number of records in CJIS databases, how do you safeguard Americans' privacy and civil liberties?**

**Cuthbertson:** We balance civil liberties with everything we do. It's important to remember that we only retain information related to a person's criminal history based on lawful contacts with law enforcement. We don't retain files on employment checks, for instance. By law, even gun background checks that come to us through NICS are destroyed every night—unless the purchase was lawfully denied. There are many similar protections in place to protect the privacy of American citizens.

# A Year of Records for CJIS

## Part 2: Cutting-Edge Technology Fuels Growth

*Part 2 of an interview with Special Agent David Cuthbertson, assistant director of the FBI's Criminal Justice Information Services Division (CJIS).*

**Q: Since its creation in 1992 as the FBI's central repository for criminal justice information, CJIS has experienced tremendous growth. To what do you attribute this success?**

**Cuthbertson:** There is no question that our success is fueled by collaboration with our partners. We rely on participating agencies for data, and we organize, store, and share that data nationwide. This collective effort helps everyone leverage invaluable crime-fighting resources. Our annual Uniform Crime Report, for example, produces crime statistics that police agencies and public administrators rely on to make decisions about how they run their cities. The 2011 report included data from more than 18,000 law enforcement agencies. That's just one of many programs that illustrate our collaborative partnerships.

**Q: How has technology contributed to the success of CJIS?**

**Cuthbertson:** A few years ago, 70,000 requests per day for fingerprint checks broke records. Now we're seeing about 140,000 requests per day. That has everything to do with technology. We recently implemented a new fingerprint-matching algorithm that improved our reliability numbers from 92 percent to 99 percent. That's a significant increase in accuracy, and for police officers on the street it translates into a greater ability to identify an individual claiming to be a different person. We continue to build our systems with next-generation technology and have made billion-dollar enhancements to our biometrics program, adding facial recognition and iris scan systems to our state-of-the-art fingerprint capabilities.

**Q: CJIS has a number of biometrics initiatives. Can you explain them?**

**Cuthbertson:** Our Biometric Center of Excellence represents the FBI's investment in staying current with emerging technologies. Leveraging our academic partnerships with West Virginia University and other institutions, the center supports and analyzes new research so that we can take these cutting-edge technologies and use them operationally. On the international front, CJIS serves in an advisory role to foreign governments that are either developing biometrics systems from the ground up or expanding existing systems. We work closely with the U.S. Departments of State and Homeland Security to put biometrics agreements in place with foreign governments that will guarantee interoperability. Here at home, we have partnered with the Department of Defense to build a Biometrics Technology Center on our campus in Clarksburg, West Virginia. The center is under construction and scheduled for completion in the spring of 2014. It will be a tremendous resource to carry us into the future.

**Q: What else can we expect from CJIS in the future?**

**Cuthbertson:** We are well-positioned for success going forward. I anticipate expansion of our legally mandated biometrics and identity verification programs regarding visa issuance and other areas related to foreign travel. We need to continue to help states and federal agencies that protect the nation's borders. We are also expanding our systems to include latent palm print functionality. Beginning next year, the FBI will have the ability to search palm prints for the first time. Studies have shown that a significant percentage of crime scene marks or latent prints are actually palm prints. With this enhancement to our systems, we will identify more criminals. We are very proud of the work being done at CJIS and look forward to continued success in the future.

Left: Members of the Memphis Evidence Response Team found bone fragments at this muddy search site, which helped turn a missing person case into a murder investigation.

# From Missing Person to Murder Victim

## Strong Partnerships Help Solve Rural Tennessee Case

When the missing person report was filed for Rose Goggins, a 21-year-old mother who lived with her fiancé's parents in rural Tennessee, the response was immediate: local police, firefighters, rescue squads, and volunteers began an intensive search using floodlights and bloodhounds. Along the banks of the Tennessee River on that cold night in January 2010 where the search was concentrated, it looked like a military encampment.

**It was Goggins' fiancé's father—the grandfather of her 11-month-old son—who called in the missing person report. But officers from the Wayne County Sheriff's Department soon began to doubt Steven Beersdorf's story.** At the request of local authorities, our agent on the scene called in the FBI's Evidence Response Team (ERT) from our Memphis office to conduct a different kind of search.

Working in the cold and snow with local law enforcement, ERT members found flesh and small bone fragments, including a palm-sized piece of skull, on the Beersdorf property, providing critical clues that Goggins was not missing, but had been murdered—while her fiancé, a National Guard reservist, was training in Mississippi for deployment to Iraq.

"Beersdorf took extraordinary steps to dispose of the body," said Special Agent Brian Fazenbaker, who works out of our Memphis office and covers eight southern counties in Middle Tennessee. It was the painstaking work of ERT members that helped move the investigation forward, "but more than anything," Fazenbaker added, "this case is a classic example of how local, state, and federal agencies work together to solve cases, each providing their own expertise."

In this case, ERT's highly trained members provided the evidence, and the Tennessee Bureau of Investigation used it to identify Goggins' remains through a DNA match. The FBI also provided a victim specialist to work with members of Goggins' family who lived out of state.

"I encourage all law enforcement agencies here to work together," said Mike Bottoms, district attorney general for the 22nd Judicial District of Tennessee, who prosecuted the Goggins case. "In a rural area, you have to work together because out here, no one is completely self-sufficient."

**"Investigations can be different in rural settings," Fazenbaker added. "You might be 120 miles from your office, and you have to depend on your local partners—and you know they are depending on you."**

A few days after the missing person report, Beersdorf and his wife were arrested and charged with first-degree murder. Beersdorf later confessed to strangling Goggins. There had been friction in the house, Beersdorf told investigators, and on that January day it spilled over into a fight that cost Goggins her life. Last March, rather than stand trial, the couple pled guilty. Beersdorf was sentenced to life in prison. His wife, who did not participate in the murder, received a 15-year sentence.

"The FBI was extremely helpful in this investigation," said Bottoms. "When the Bureau gets involved in a case like this," he added, "it's not just for the three or four days of searching and evidence gathering. It's also a commitment to attend court hearings and participate in a trial if it comes to that."

Fazenbaker noted that agents working in rural resident agencies "pretty much handle whatever cases come in the door. Out here in these small communities," he said, "we are proud of the fact that we can really make a difference."

# Mafia Family Fraud

## The Case of the Stolen Company

It's a criminal's dream—owning a financial company that can be looted at will. That's just what 13 individuals—including two with ties to organized crime families—are accused of in a federal indictment announced last month in New Jersey.

Among those charged in the 25-count indictment is Nicodemo Scarfo—a member of the Lucchese crime family and son of Nicodemo Scarfo Sr., the imprisoned former boss of the Philadelphia La Cosa Nostra (LCN) crime family. Also charged were Salvatore Pelullo—an associate of the Lucchese and Philadelphia LCN families—and 11 others…all in connection with an alleged criminal takeover of FirstPlus Financial Group (FPFG), a publicly held company based in Texas. The takeover resulted in honest FPFG shareholders losing at least $12 million; the company ultimately filed for bankruptcy.

The group was charged with various crimes in connection with this racketeering conspiracy, including securities fraud; wire, mail, and bank fraud; extortion; money laundering; and obstruction of justice. In addition to Scarfo and Pelullo, other members of the criminal enterprise included five attorneys, a certified public accountant, and Scarfo's wife.

**How did they do it?** According to the indictment, members of the criminal enterprise devised a plan in 2007 to take over FPFG by replacing its board of directors and management with individuals who would serve at the direction of Scarfo and Pelullo. To accomplish this, they allegedly accused board members of financial improprieties that, if brought to light, would result in costly lawsuits. Eventually, through threats and intimidation, every member of the board and executive management left.

After gaining control of the company, the looting began:

- The new board approved the acquisition of "companies" owned by Scarfo and Pelullo for millions of dollars and several hundred thousand shares of FPFG stock—except that these companies were really nothing more than shell corporations and had virtually no value. Proceeds from the sale of the companies ended up in the pockets of the criminal conspirators.

- The new board also approved a number of "consulting" agreements for hundreds of thousands of dollars. This consulting work was never performed, and the proceeds went to the criminals.

Scarfo and Pelullo allegedly purchased items like expensive homes, luxury vehicles, yachts, and jewelry. And like any good mob soldiers, they also allegedly purchased weapons.

**Since FPFG was a public company, it was obligated to file reports with the Securities and Exchange Commission (SEC).** The indictment alleges that, in order to conceal the involvement of former felons Scarfo and Pelullo in the company, their henchman at FPFG filed fraudulent paperwork. Scarfo is also accused of concealing his involvement in FPFG from his probation officer—at the time of the scheme, he had been released from prison and was under federal supervision.

In addition, the indictment alleges that the Scarfo-Pelullo conspiracy was operated with the assistance and direction of members and associates of La Cosa Nostra and that some of the financial proceeds from the scheme ended up in the hands of the LCN.

**This multi-year investigation was very complex and required not only using sensitive investigative techniques, but also carefully analyzing voluminous financial records and following the money trail through various financial accounts. And we didn't do it alone—we worked with the Department of Labor's Inspector General; the Bureau of Alcohol, Tobacco, Firearms, Explosives; and the SEC.**


# Potomac River Rapist Cold Case

## Help Us Catch a Murderer and Serial Rapist

Christine Mirzayan was 29 years old, a National Academy of Sciences intern, and had a promising career ahead of her on the summer evening in 1998 when she was walking home from a cookout in Washington, D.C. Tragically, she never made it. Her killer—a serial rapist who had previously attacked eight other women—is still at large.

**Today, the FBI and its law enforcement partners are reaching out to the public—and a reward of up to $25,000 is being offered by Washington's Metropolitan Police Department (MPD)—for assistance in apprehending the offender known as the Potomac River Rapist.**


Christine Mirzayan

Between 1991 and Mirzayan's murder seven years later, the Potomac River Rapist brazenly and brutally preyed upon women in the Washington area. Victims were attacked in their homes and included an 18-year-old babysitter and a mother whose infant was in the house at the time of the attack. Seven of the nine attacks have been linked by DNA, and all are linked by the offender's similar violent methods.

"It is believed the suspect lived in, spent a considerable amount of time in, or was otherwise familiar with the areas of the attacks," said Special Agent Erin Sheridan. "The suspect is generally described as an African-American male of medium build who is currently believed to be in his 40s or 50s."

A task force—made up of the FBI, MPD, Maryland's Montgomery County Police Department, and the U.S. Attorney's Office for the District of Columbia—is working to capture the Potomac River Rapist. Using a variety of digital platforms such as FBI.gov, social media, radio spots, and digital billboards, the media campaign provides information about the case and the offender.

"We believe that someone in the public will help solve this case," Sheridan said. "Because law enforcement is in possession of DNA evidence that can either positively link the suspect to his crimes or exclude innocent parties, the public should not hesitate to provide information, even if it is just the name of a potential suspect."

Witnesses at the time of Mirzayan's murder helped artists create a composite sketch shown here that has since been age-enhanced. That individual is being sought in connection with the case.

**Most of the assaults followed a similar pattern.** "The rapist used a blitz attack, surprising his victims with force—sometimes wielding a knife or screwdriver—and throwing a blanket or towel over their heads," said Capt. David Gillespie of the Montgomery County Police Department. "He often stalked his targets, breaking into their homes and waiting, sometimes for hours, for them to come home."

"It has been more than 20 years since this predator began stalking, hunting, and sexually assaulting women," said Todd Williams, an MPD detective who is part of the Potomac River Rapist Task Force. "He became increasingly violent during these attacks and killed Christine Mirzayan by bludgeoning her with a boulder. He is extremely violent and dangerous and needs to be caught and taken off the streets."

**We need your help.** Law enforcement agencies are asking anyone with information to contact the MPD at (202) 727-9099 or the FBI at 1-800-CALL-FBI (1-800-225-5324). Additionally, anonymous information may be submitted to the police department's TEXT TIP LINE by text messaging 50411. You can also submit a tip at tips.fbi.gov.

# Preliminary Crime Stats

## For the First Half of 2011

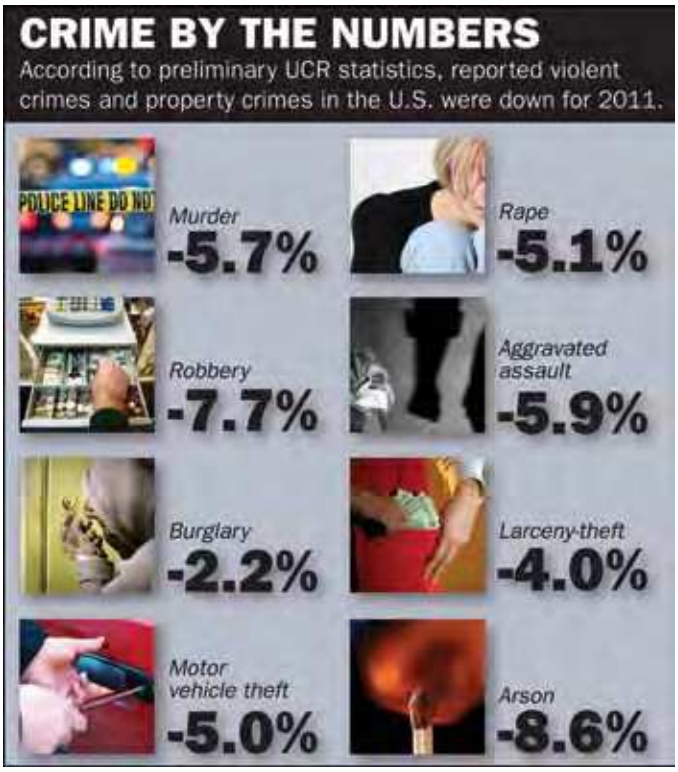
According to the FBI's just-released *Preliminary Semiannual Uniform Crime Report*—which covers January through June 2011—the number of violent crimes and property crimes reported to us showed a decrease compared to figures from the same time frame in 2010, continuing a downward trend.

Overall, violent crimes were down 6.4 percent, while property crimes fell 3.7 percent.

**Here are some highlights of our preliminary crime statistics for the first six months of 2011, as compared to the same period last year:**

- The occurrence of all four offense types in the violent crime category decreased—murder was down 5.7 percent; rape dropped 5.1 percent, robbery fell 7.7 percent, and aggravated assault declined 5.9 percent. And it didn't matter what region of the country you lived in—decreases in each category were seen in the Northeast, Midwest, South, and West.
- Overall violent crime declined in all six city population groups and metropolitan and non-metropolitan counties, with most violent crime offenses showing decreases. There were some upticks: murder in cities with populations between 500,000 and 999,999 (up 1.2 percent); murder in cities with under 10,000 people (2.6 percent); rape in cities of 1 million or more (1.0 percent); rape in cities of 500,000 to 999,999 (6.7 percent); and rape in cities of 250,000 to 499.999 (0.1 percent).
- Like violent crime, all offense types in the property crime category showed decreases—burglary (down 2.2 percent), larceny-theft (4.0 percent), and motor vehicle theft (5.0 percent). And like violent crime, these declines occurred in all four regions of the country.
- All three property crime types fell in all six city population groups and in metropolitan counties. Just one exception in non-metropolitan counties—larceny-theft was up 0.5 percent.
- Arson, which declined 8.6 percent overall, also saw individual decreases in all four areas of the country and in every population group.

**Uses for the UCR data:** To provide law enforcement with data that can help with budget formulation, planning, resource allocation, assessment of police operations, etc., to help address crime problems at various levels.




Also, criminal justice researchers can study the nature, cause, and movement of crime over time. Legislators can draft anti-crime measures using the research findings and recommendations of law enforcement administrators, planners, and public and private entities concerned with the problem of crime. Chambers of commerce and tourism agencies can examine the data to see how it impacts the geographic jurisdictions they represent. And the news media can use crime statistics to inform the public about the state of crime locally and nationally.

**What this UCR data should not be used for:** To compile rankings of individual jurisdictions and institutions of higher learning and/or to evaluate the effectiveness of individual law enforcement agencies. These incomplete analyses have often created misleading perceptions that adversely affect geographic entities and their residents. UCR statistics include only jurisdictional population figures along with reported crimes, clearance, or arrest data—not the many socio-economic and other factors that cause the volume and type of crime to vary from place to place.

The preliminary full-year crime statistics will be released next summer, and the final Crime in the United States 2011 report will be available in the fall.


Left: Geocoordinates are embedded in the image, which was transmitted via a smartphone. The data make it easy to plot the sender's location on a map.

# Cyber Alerts for Parents & Kids

## Tip #1: Be Prudent When Posting Images Online

With the explosive popularity of smartphones and social media platforms, sharing photos has never been easier. Millions of pictures are uploaded to the web every day, and camera-enabled mobile phones are the perennial top-selling consumer electronic devices. So it's a safe bet that even more photos will be cropping up on image-hosting communities and personal websites.

But what exactly is being shared?

**In some cases, you might unwittingly be letting others know where you live and work and your travel patterns and habits.** These details can be revealed through bits of information embedded in images taken with smartphones and some digital cameras and then shared on public websites. The information, called metadata, often includes the times, dates, and geographical coordinates (latitude and longitude) where images are taken.

While the geospatial data can be helpful in myriad web applications that plot image locations, it also opens a door for criminals, including burglars, stalkers, and predators. It's not a stretch to imagine young teens' images of their ventures to the mall or beach being culled by web predators and meticulously plotted on online maps.

"It's not something we think is happening. We know it's happening," said Kevin Gutfleish, head of the Innocent Images Intelligence Unit in the FBI's Cyber Division. The unit provides analysis and assessments of emerging threats for the operational arm of the Innocent Images National Initiative, which targets child pornography and sexual predators.

"The way that images are being posted in real time allows others who have access to see the metadata and see where the photos were taken and reveal their location at that time," Gutfleish said.

An intelligence analyst in the FBI Criminal Division's Crimes Against Children Unit said these details can reveal a "pattern of life," particularly when images posted over time are clustered in geographic locations.

"It doesn't have to be in real time to be dangerous," said the analyst. "Historical data can tell you a lot about individuals' day-to-day habits and may indicate where they are most likely to be at a certain time."

Some popular social media sites automatically scrub metadata from images before they are published. On the other hand, some leverage the data to display location information beside the images. An amateur sleuth could easily pinpoint a location using the available latitude and longitude coordinates.

"Even if they don't intentionally say where they are, the photos could reveal that," Gutfleish said. "And that could present a potential danger."

**Gutfleish said he has seen an increase in intelligence reports and complaints about the potential misuse of the metadata embedded in photos.** He said the proliferation of online tools that aggregate personal information from social networking and image hosting sites is enough to urge a level of caution.

He suggests mobile phone users at the very least check the "options" or "settings" on their phones (and any applicable mobile applications) to see if they are sharing location information. In many cases, the default setting is to share location information.

"It's just a best-practice if you don't want to give out your location," Gutfleish says. "We simply want to make sure people know this is happening."

*This story is the first in an occasional series aimed at providing practical web advice and tips for parents and their kids.*

# The Year in Review

## A Look at FBI Cases, Part 1

The FBI conducted thousands of investigations in 2011, from terrorists bent on murder and cyber thieves hacking networks to corrupt government officials and fraudsters stealing billions of dollars from innocent victims.

As the year comes to a close, here is a look at some of the most significant cases the Bureau investigated with the help of our domestic and international law enforcement and intelligence community partners.

**Part 1 focuses on our top investigative priority: protecting the nation from terrorist attack.** The death of Osama bin Laden in May was a milestone, but al Qaeda remains committed to high-profile attacks against the U.S. And on the home front, lone offenders radicalized on the Internet continue to pose a serious threat to national security.

Here are some of the top terror cases of 2011, in reverse chronological order:

**Murder of U.S. soldiers in Iraq:** A 38-year-old Canadian citizen was indicted this month by a New York grand jury for his role in the murder of five American soldiers in a suicide-bomb attack in Iraq in 2009. The individual was arrested last January in Canada, and the U.S. is seeking his extradition.

**Indictment of senior citizens in ricin plot:** Four Georgia men in their 60s and 70s were arrested last month for planning to manufacture the biological toxin ricin and purchasing explosives for use in attacks against American citizens. The defendants are alleged to be part of a fringe militia group.

**Plot against Saudi ambassador:** Two individuals were charged in October for their participation in a plot directed by elements of the Iranian government to murder the Saudi ambassador to the U.S. with explosives while the ambassador was on U.S. soil. One of the individuals is in custody; the other is still at large.

**Attack planned on U.S. Capitol:** A 26-year-old Massachusetts man was arrested in September and charged with plotting to bomb the Pentagon and U.S. Capitol using remote-controlled aircraft filled with explosives.

**Material support to terrorists:** An Albanian citizen living in New York was charged in September with providing material support to terrorists for planning travel to Pakistan to join a radical jihadist fighting group. He was arrested while trying to catch a flight out of the country.


**Texas bomb plot:** A 21-year-old soldier who was absent without leave was charged in July with planning to detonate a bomb inside a restaurant frequented by soldiers from Fort Hood. When he was arrested, the individual was in possession of a variety of bomb-making components. In November he was charged with additional crimes including attempted murder.

**Plot to attack Seattle military installation:** Two men were indicted in July for conspiring to use a weapon of mass destruction to attack a military installation in Seattle with the intention of killing U.S. citizens. Law enforcement first became aware of the plot when an individual alerted them that he had been approached about participating in the attack.

**Conduit to terror:** A Somali national in his mid-20s was indicted in July for providing material support to foreign terror organizations al Shabaab and al Qaeda in the Arabian Peninsula (AQAP). He was captured in the Gulf region by the U.S. military in April 2011 and was allegedly a conduit between al Shabaab and AQAP.

**Iraq bomb attacks:** An Iraqi citizen who allegedly carried out numerous improvised explosive device (IED) attacks against U.S. troops in Iraq and another Iraqi national alleged to have participated in the Iraq insurgency were indicted in May on terrorism charges in Kentucky, where both were residents.

**Jihadist indictment:** A 20-year-old Saudi Arabia citizen and Texas resident was arrested in February and charged with attempted use of a weapon of mass destruction in connection with the purchase of chemicals and equipment used to make an IED and his research of potential U.S. targets. The individual came to the U.S. in 2008 on a student visa.


# The Year in Review

## A Look at FBI Cases, Part 2

With our partners in the law enforcement and intelligence communities, the FBI worked thousands of investigations during 2011, from cyber and hate crimes to public corruption and multi-million-dollar fraud schemes. As the year draws to a close, we take a look back at some of 2011's most significant cases.

**Part 1 focused on terrorism. This segment highlights some of the year's top cases from the FBI's other investigative priorities:**

**Martin Luther King Jr. Day attempted bombing:** A Washington state man was sentenced to 32 years in prison last week for attempting to bomb a Martin Luther King Jr. Day parade last January in Spokane.

**International cyber takedown:** Six Estonian nationals were arrested last month for running a sophisticated Internet fraud ring that infected millions of computers worldwide with a virus and enabled the thieves to manipulate the multi-billion-dollar Internet advertising industry.

**Operation Delta Blues:** After a two-year investigation dubbed Operation Delta Blues, 70 individuals—including five law enforcement officers—were charged in Arkansas in October with crimes including public corruption, drug trafficking, money laundering, and firearms offenses.

**Corporate fraud scheme:** The former chairman and owner of Taylor, Bean & Whitaker (TBW), a privately held mortgage lending company, was sentenced in June to 30 years in prison for his role in a more than $2.9 billion fraud scheme that contributed to the failure of TBW and Colonial Bank, one of the 25 largest banks in the U.S.

**James "Whitey" Bulger arrest:** Top Ten fugitive James "Whitey" Bulger was arrested in June thanks to a tip from the public—just days after a new FBI media campaign was launched to help locate the Boston gangster who had been on the run for 16 years.

**Cyber fraud organization disruption:** In an unprecedented move in the fight against cyber crime, the FBI disrupted an international cyber fraud operation in April by seizing the servers that had infected as many as two million computers with malicious software.

**Southwest border gang arrests:** Thirty-five members and associates of the Barrio Azteca gang were charged in March with various counts of racketeering, murder, drug offenses, and money laundering. Ten of the defendants were Mexican nationals and were also charged in connection with the 2010 murders in Juarez, Mexico of a U.S. Consulate employee, her husband, and the husband of a U.S. Consulate employee.

**Health care fraud takedown:** Twenty individuals, including three doctors, were charged in South Florida in February for their participation in a fraud scheme involving $200 million in Medicare billing for mental health services. The charges coincided with a national federal health care fraud takedown involving 111 defendants in nine cities.

**Selling secrets for profit:** A 66-year-old resident of Hawaii was sentenced in January to 32 years in prison for communicating classified national defense information about U.S. military planes to the People's Republic of China, along with illegally exporting military technical data and other offenses.

**Massive Mafia takedown:** Nearly 130 members of the Mafia in New York City and other East Coast cities were arrested in January in the largest nationally coordinated organized crime takedown in FBI history. Charges included murder, drug trafficking, arson, loan sharking, illegal gambling, witness tampering, labor racketeering, and extortion.

# 2011: The FBI Story Index

# 2011: The FBI Story Index



## Cyber Crimes



## Director/FBI Leadership



## Field Cases

# 2011: The FBI Story Index



## Foreign Counterintelligence



## General

# 2011: The FBI Story Index



## History



## Intelligence



## International

# 2011: The FBI Story Index



## Lab/Operational Technology



## Major Thefts/Violent Crime



## Organized Crime/Drugs

# 2011: The FBI Story Index



## Partnerships

# 2011: The FBI Story Index

# 2011: The FBI Story Index

**FBI OFFICE OF PUBLIC AFFAIRS**
935 Pennsylvania Avenue NW
Washington, DC 20535


Washington Field Office Special Agent in Charge Brenda Heck—wearing an FBI JTTF (Joint Terrorism Task Force) jacket—at a news conference in June 2011 concerning a suspicious vehicle found near the Pentagon. Joining her are partners from the Arlington Police Department (left) and U.S. Park Police (right). AP Photo/Alex Brandon.