



# 2012 The FBI Story



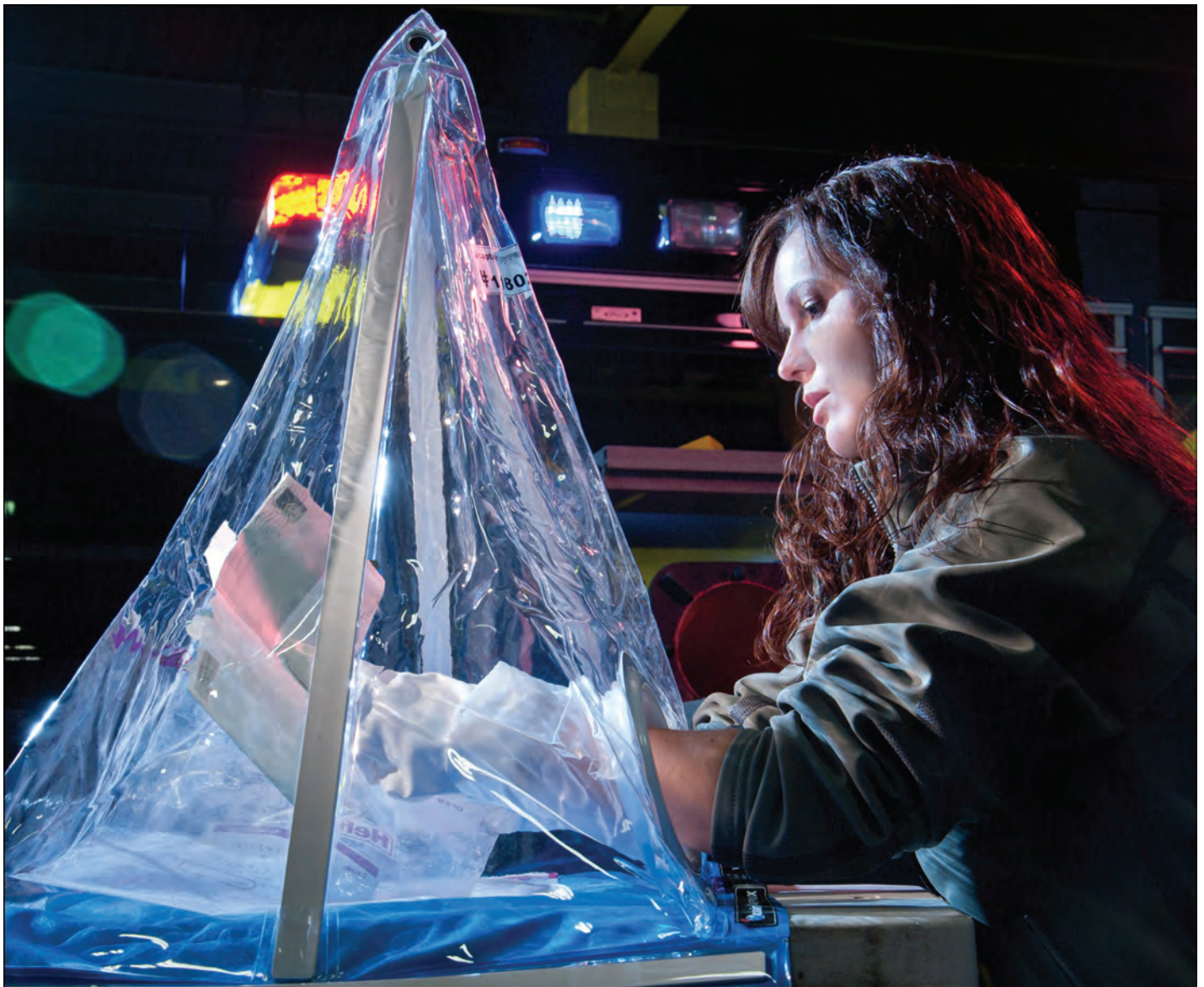
The Strategic Information and Operations Center at FBI Headquarters is the 24/7 command post that monitors FBI operations and law enforcement activities around the globe.



---

**2012**

# The FBI Story



An FBI agent examines a potentially contaminated letter during a white powder training exercise.

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

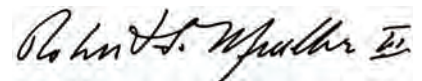
For the FBI and its partners, 2012 was a year that reminded us once again of the seriousness of the security threats facing our nation.

During the year, extremists plotted to attack—unsuccessfully, thanks to the work of our Joint Terrorism Task Forces—the U.S. Capitol, the New York Federal Reserve Bank, and other landmarks on U.S. soil. Tragically, on the 11th anniversary of 9/11, a hateful attack in Benghazi took the lives of the U.S. Ambassador to Libya and three other Americans. In the cyber realm, a rising tide of hackers took electronic aim at global cyber infrastructure, causing untold damages. High-dollar white-collar crimes of all kinds also continued to siphon significant sums from the pocketbooks of consumers. And in Newtown, Connecticut, 20 young children and six adults lost their lives in one of the worst mass shootings in American history, ending a year of violence that saw similar tragedies around the country.

Working with its colleagues around the globe, the FBI is committed to taking a leadership role in protecting the nation. As you can see from this book—an annual compilation of stories from the FBI's public website that provides a snapshot of Bureau milestones, activities, and accomplishments—we used the full range of our intelligence, investigative, and operational skills to address major threats during the year. We helped avert terrorist attacks and derail terrorist supporters, put cyber criminals and fraudsters behind bars, and dismantled violent gangs and organized crime groups.

Today, as these pages make clear, protecting our country and our communities is truly a team effort. National security and law enforcement organizations are working together more closely than ever. At the same time, Americans from all walks of life can and do make a difference in solving and preventing crime and terrorism. Businesses can become aware of the warning signs of insider economic espionage (page 39). Community leaders can learn about such scourges as human trafficking (page 6). Consumers can get wise to online scams like the Reveton virus (page 66). Teachers can educate their students about cyber safety through our new Safe Online Surfing website (page 85). And citizens can contact us with tips and leads in our investigations, such as our search for a college student's killer (page 50).

I want to thank all of you for your support and leadership, which is so vital to the success of the FBI. And I wish you all the best in the months and years ahead.



Director Mueller at the U.S. Embassy in Estonia during a trip in early 2012 to strengthen partnerships in Northern Europe.  
Photo courtesy of the U.S. Embassy.



## Overcoming the Language Barrier

### Translation Center at the Ready to Assist U.S. Intelligence

At the National Virtual Translation Center's offices near FBI Headquarters in Washington, it feels like a mini United Nations, with linguists working in Chinese, Arabic, and other languages. The real global reach of the organization, however, is not its brick and mortar presence but rather the virtual capability reflected in its name.

**Language specialists around the country—some working in secure government locations and others working from their homes—translate a variety of foreign-language material that aids the U.S. intelligence community and helps protect national security.**

Established by Congress in 2003 with the FBI as its executive agency, the center—known by its NVTC acronym—is a collaborative government organization in the Office of the Director of National Intelligence, but it functions more like a nimble private-sector company that can staff up to respond to its customers' immediate needs.

Linguists working part time and full time on a contract basis may be called on to translate a variety of material—such as a 500-page technical document, an audio cassette, or a propaganda pamphlet—in any of 100 different languages or dialects.

All NVTC linguists are U.S. citizens who have passed a thorough background investigation conducted by the FBI, and they come from all walks of life. They include students, business professionals, and even stay-at-home moms. Often, English is not their first language.

"We are an elastic workforce," said NVTC Director Mary Ellen Okurowski, explaining that the center operates on a fee-for-service business model. "We support our customers in the U.S. intelligence community on their terms," she said. "So we have to provide quality work on time or they will simply not come to us."

**Like many members of the intelligence community, the FBI relies on its own linguists for much of the organization's translation needs. But when the Bureau or another agency is faced with too much raw material and too little time to translate it—or it needs language expertise it does not possess—NVTC gets the call.**



The center's linguists rarely know the agency they are translating for or the reason for the translation request. Doug Kouril, the center's director of operations, noted that although NVTC language specialists may offer cultural perspectives with their translations—which can have a bearing on meaning—they do not collect or provide analysis.

During the past several years, the demand for NVTC's expertise has increased significantly, according to the FBI's Pamela Hobson, the center's director of administration. In fiscal year 2010, for example, NVTC linguists translated nearly 209,000 pages and more than 1,000 hours of audio material, doubling output from the previous year.

Customers can efficiently request work directly from NVTC's website, and the center's sophisticated quality control program monitors the work at every step of the way. "Our potential for growth is strong," Hobson added, "because we are always there when our customers need us."

"NVTC is a living model of inter-agency collaboration," Okurowski said. "We look forward to continuing to provide a high level of service to our customers. Our goal is to make NVTC an indispensable resource for the intelligence community."



## Malware Targets Bank Accounts

### ‘Gameover’ Delivered via Phishing E-Mails

Cyber criminals have found yet another way to steal your hard-earned money: a recent phishing scheme involves spam e-mails—purportedly from the National Automated Clearing House Association (NACHA), the Federal Reserve Bank, or the Federal Deposit Insurance Corporation (FDIC)—that can infect recipients’ computers with malware and allow access to their bank accounts.

The malware is appropriately called “Gameover” because once it’s on your computer, it can steal usernames and passwords and defeat common methods of user authentication employed by financial institutions. And once the crooks get into your bank account, it’s definitely “game over.”

Gameover is a newer variant of the Zeus malware, which was created several years ago and specifically targeted banking information.

**How the scheme works:** Typically, you receive an unsolicited e-mail from NACHA, the Federal Reserve, or the FDIC telling you that there’s a problem with your bank account or a recent ACH transaction. (ACH stands for Automated Clearing House, a network for a wide variety of financial transactions in the United States.) The sender includes a link in the e-mail that will supposedly help you resolve whatever the issue is. Unfortunately, the link goes to a phony website, and once you’re there, you inadvertently download the Gameover malware, which promptly infects your computer and steals your banking information.

After the perpetrators access your account, they conduct what’s called a distributed denial of service, or DDoS, attack using a botnet, which involves multiple computers flooding the financial institution’s server with traffic in an effort to deny legitimate users access to the site—probably in an attempt to deflect attention from what the bad guys are doing.

**But that’s not the end of the scheme:** Recent investigations have shown that some of the funds stolen from bank accounts go towards the purchase of precious stones and expensive watches from high-end jewelry stores. The criminals contact these jewelry stores, tell them what they’d like to buy, and promise they will wire the money the next day. So the next day, a person involved in the money laundering aspect of the crime—called a “money mule”—comes into the store to pick up the merchandise. After verifying that the money is in the store’s account, the jewelry is turned over to the mule, who then gives the items to the organizers of the scheme or converts them to cash and uses money transfer services to launder the funds.

In many cases, these money mules are willing participants in the criminal scheme. But increasingly, as part of this scheme, we see a rising number of unsuspecting mules hired via “work-at-home” advertisements who end up laundering some of the funds stolen from bank accounts. The criminals e-mail prospective candidates claiming to have seen their résumés on job websites and offer them a job. The hired employees are provided long and seemingly legitimate work contracts and actual websites to log into. They’re instructed to either open a bank account or use their own bank account in order to receive funds via wire and ACH transactions from numerous banks...and then use money remitting services to send the money overseas.

If you think you’ve been victimized by this type of scheme, contact your financial institution to report it, and file a complaint with the FBI’s Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov).

# Closing a 'Crime Superstore'

## Not-So Garden Variety Fraud in the Garden State

They hijacked identities on the other side of the globe... faked drivers' licenses and other documents...built bogus credit histories and boosted the scores in clever ways... then used it all to open bank accounts and credit lines they could loot at will.

In the end, they created what our Newark Special Agent in Charge Mike Ward called a "crime superstore"—a sophisticated way to rob financial institutions, retailers, car leasing companies, and even the IRS out of millions of dollars.

**Following an undercover investigation led by the FBI and its partners, it all came crashing down in September 2010, when 43 members of the criminal ring were charged in this complex scheme.** Another 10 individuals were charged for various related offenses at the same time during a coordinated takedown. And on Monday, the leader of the band of thieves—San-Hyun Park, known to his criminal colleagues as "Jimmy"—pled guilty in federal court in Newark.

The Park criminal enterprise started by stealing Social Security numbers from unsuspecting individuals—usually from China—who were employed in American territories in Asia like Saipan, Guam, and the Philippines. These identities were then sold to customers in the U.S. for \$5,000 to \$7,000. Although the stolen identities were Chinese, the vast majority of Park's customers were Korean-Americans. The ring would use the phony Social Security numbers to obtain authentic driver's licenses, identification cards, and other identity documents from various states...or manufacture counterfeit licenses and other documentation.

**Based in Bergen County, New Jersey, Park's organization was subdivided into different cells, each with a unique role.** First, there were the customers who paid Park and his co-conspirators for fake identity documents. Then, there were the brokers, suppliers, and manufacturers of the phony identity documents—like Social Security cards, immigration documents, and driver's licenses. A third group included merchants who colluded with the organization by knowingly swiping phony credit cards in return for a fee called a *kkang*. The credit card buildup



teams made up the fourth group, fraudulently inflating credit scores to help open the bank and credit accounts.

The buildup teams would take one of the stolen Social Security numbers—and the Chinese identity attached to it—and add that person's name as an authorized user to other co-conspirators' credit card accounts. These co-conspirators, who knew their accounts were being used to commit fraud, received a fee for their service.

After the credit buildup was completed, the Park criminal enterprise conspired with its customers to use the fraudulent identities to apply for checking accounts, bank and retail credit cards, debit cards, lines of credit, and loans. Members of the criminal conspiracy used their sizeable proceeds to live large, buying such luxury items as fancy cars, expensive liquor, and designer shoes.

**The multi-agency investigation made use of cooperating witnesses and an undercover federal agent, as well as court-authorized wiretaps, to record incriminating conversations among members of the crime ring and others.** The FBI partnered with several federal agencies and local police departments in New Jersey, among others. We also worked cooperatively with the major banks, credit card companies, and department stores targeted by this criminal organization.





Left: On January 17, 2011, as hundreds of people gathered in downtown Spokane to participate in the Martin Luther King, Jr. Day Unity March, Kevin Harpham placed a backpack bomb (inset) along the parade route on Main Avenue. The graphic shows the likely direction of the blast had the bomb detonated.

## MLK Parade Bomber

### Horrific Hate Crime Prevented; Case Solved

Had his homemade bomb gone off—one he had diabolically constructed using shrapnel coated with a substance meant to keep blood from clotting in wounds—Kevin Harpham would have undoubtedly caused the death and injury of many people at the Martin Luther King, Jr. Day Unity March in Spokane, Washington in 2011.

Instead, Harpham was eventually caught and recently sentenced to 32 years in prison for a hate crime and other offenses related to the attempted bombing. The case illustrates how a quick response by citizens and local law enforcement averted a tragedy and how teamwork and time-tested investigative techniques led to the apprehension of an individual who has shown no remorse for his actions.

**“Clearly he intended to detonate the device, cause mass carnage, and then survey the devastation,”** said Special Agent Frank Harrill, who supervised the investigation. **“Harpham was acting out against what he termed multiculturalism, but his hatred was firmly rooted in violent white supremacy. This was a prototypical hate crime.”**

On January 17, 2011, as hundreds of people gathered in downtown Spokane to participate in the march, Harpham placed his backpack bomb along the parade route at Washington Street and Main Avenue. Alert city workers discovered the suspicious backpack before the march started, and Spokane Police Department officials changed the route as a precaution. The Spokane Police and Sheriff’s Office bomb squad was called in, and their precision in disarming the device enabled evidence to be

preserved that would help lead FBI agents to Harpham.

The FBI’s Joint Terrorism Task Force (JTTF) in Spokane immediately began an investigation, and JTTF members canvassed the region for batteries and other components similar to those used in the bomb. Within a month, in a small town about 60 miles north of Spokane, they discovered that a local outlet of a large retail chain was selling the same kind of fishing weights Harpham had used as shrapnel.

Store records showed there had been three large purchases of the weights in recent months—two were paid for in cash, but a debit card was used in one transaction, and it belonged to Harpham. At the same time, the FBI Laboratory had been working to extract a DNA sample from the backpack that was later matched to Harpham through his military records.

**Investigators also learned of Harpham’s white supremacy postings on the Internet and his affiliation with a neo-Nazi group called the National Alliance.**

Because he lived in a remote, relatively inaccessible area and was likely heavily armed, our Hostage Rescue Team devised a ruse to lure Harpham out of his house. He was arrested March 9, 2011 without incident—but as agents suspected, he was armed when taken into custody.

“Kevin Harpham was the lone wolf that all of us in law enforcement dread,” Harrill said. “He lived alone, he worked alone, and he didn’t foreshadow the bombing plot in any meaningful way. He targeted those who were attempting to celebrate an event meant to unite society,” Harrill added, “and he was prepared to indiscriminately kill men, women, and children.”

Harrill credited teamwork and strong partnerships for stopping Harpham and bringing him to justice. “From the workers who noticed the device to the police response, the JTTF investigation, the expertise of the FBI Laboratory, and the prosecuting skill of the U.S. Attorney’s office—everything worked just as it should have.”

# A Mother's Worst Nightmare

## Fusion Center Key in Rescue of Abducted Infant

On a September evening in 2009, a woman answered a knock at her Nashville, Tennessee door from someone claiming to be an immigration agent. A short time later, when police responded to a 911 call from the residence, they found the woman beaten and stabbed—and her 4-day-old son abducted.

The Metropolitan Nashville Police Department (MNPd) requested assistance from the FBI and the Tennessee Bureau of Investigation (TBI), and a command post was established at TBI's Tennessee Fusion Center, where investigators from all three agencies began working around the clock to locate the missing infant.

**“There was a tremendous sense of urgency about the case,” said Special Agent Eric Brown, who works in the FBI's Nashville Resident Agency out of the Memphis Field Office. “Everyone feared for the life of the child.”**

Initially, all that investigators had to go on was the mother's description of the kidnapper, who had seriously injured her during the attack and abduction. While fusion center personnel began responding to AMBER Alert tips coming in from around the country, Brown and others learned from the victim that she had visited a food assistance center and stopped at a local big-box store before returning home on the day of the kidnapping.

MNPd detectives immediately requested and received surveillance video from the store. “In the parking lot video, we could see that a car appeared to be mimicking the movements of the car the victim was in,” Brown said. “When her car pulled in, the other car pulled in. When she pulled out, the other car pulled out and followed.”

The video also revealed a partial, grainy license plate image that was sent to a lab for enhancement. Because of the urgency of the case, the lab work that might have taken days to complete took only hours—and it showed a more complete tag number as well as a state: Indiana.

**Fusion center and FBI analysts worked to narrow the possibilities and eventually came up with a vehicle owned by a rental car company.** At the company's airport rental counter, surveillance video showed that the woman who rented the car in question fit the description



**Surveillance video from a store visited by the victim revealed a grainy Indiana license plate, which fusion center and FBI analysts ultimately linked to a vehicle rented by the suspect.**

of the kidnapper. The car company also provided credit card and contact information for the renter, Tammy Silas, who lived just across the Tennessee line in Alabama.

Silas' credit card transactions put her close to the victim's house at the time of the abduction. Investigators also obtained bank surveillance video showing her withdrawing money from a nearby ATM—and a baby car seat could clearly be seen next to her in the passenger seat.

**The kidnapping took place on a Tuesday evening, when Silas knocked on the victim's door pretending to be an immigration official. That Friday night, investigators knocked on Silas' door in Alabama, arrested her, and recovered the baby—now 6 days old—unharm.**

“Tammy Silas had a desire to have a baby,” Brown said, “and she went to great lengths to obtain one, even if it meant kidnapping and assaulting the mother.” Silas pled guilty to kidnapping last February and is currently serving a 20-year prison sentence.

“We were able to solve this case so quickly because all the agencies involved worked together and brought their own expertise to the investigation,” said Sgt. Daniel Postiglione, a veteran MNPd investigator. “We were all very thankful to get the baby back to his mother in so short a period of time.”





## Human Trafficking Prevention

### Help Us Identify Potential Victims

For the young Ukrainians, it was a dream come true—the promise of well-paying jobs and free room and board in the United States. Once they arrived, however, it quickly turned into a nightmare. They were forced to endure 16-plus hour workdays, usually with no pay. Their living conditions were wretched, with up to 10 workers in often-unfurnished apartments or row houses. And they faced intimidation, threats of physical harm, or actual violence to keep them in line.

Members of the criminal enterprise responsible for these workers' misery were ultimately identified and charged in a conspiracy to operate a human trafficking scheme. But, as we observe National Slavery and Human Trafficking Prevention Month, we're reminded that there are still thousands of victims in the U.S.—and millions worldwide—being forced into both legal and illegal activities.

**Human trafficking generates billions of dollars of profit each year, making it one of the world's fastest growing criminal activities.** The FBI investigates it as a priority under our civil rights program, but we see human trafficking activities in other areas as well, including organized crime, crimes against children, and gangs.

To address the threat, we work cases with our local, state, federal, and international partners and participate in approximately 70 multi-agency human trafficking task forces. We also offer our counterparts—as well as non-governmental organizations, including non-profits—human trafficking awareness training. And to help get a better handle on the issue within the U.S., the FBI's Uniform Crime Reporting program plans to start collecting human trafficking data from law enforcement in 2013.

Many of our human trafficking cases are based on information from our partners and from criminal sources, but we also can and do receive tips from the public.

**That's where you come in.** Please keep your eyes out for the following indicators that suggest the possibility of human trafficking:

- Individuals who have no contact with friends or family and no access to identification documents, bank accounts, or cash;
- Workplaces where psychological manipulation and control are used;
- Homes or apartments with inhumane living conditions;
- People whose communications and movements are always monitored or who have moved or rotated through multiple locations in a short amount of time;
- Places where locks and fences are positioned to confine occupants; and
- Workers who have excessively long and unusual hours, are unpaid or paid very little, are unable take breaks or days off and have unusual work restrictions, and/or have unexplained work injuries or signs of untreated illness or disease.

Bear in mind: human trafficking victims can be found in many job locations and industries—including factories, restaurants, elder care facilities, hotels, housekeeping, child-rearing, agriculture, construction and landscaping, food processing, meat-packing, cleaning services...as well as the commercial sex industry.

**Here's one more thing to consider:** while the majority of human trafficking victims in our cases are from other countries and may speak little or no English, approximately 33 percent of victims are Americans. They come from a variety of groups that are vulnerable to coercive tactics—like minors, certain immigrant populations, the homeless, substance abusers, the mentally challenged and/or minimally educated, and those who come from cultures that historically distrust law enforcement or who have little or no experience with the legal system.

If you suspect human trafficking activities, do us and the victims a big favor: call the National Human Trafficking Resource Center at 1-888-373-7888 or submit a tip at <https://tips.fbi.gov>.

# A Byte Out of History

## Closing in on the Barker/Karpis Gang

In January 1935—77 years ago this month—more than a dozen Bureau agents surrounded a quaint two-story home on Lake Weir, Florida. Within moments, a fierce shoot-out erupted. It didn't go well for the heavily armed criminals inside.

**For the Bureau of Investigation—just six months away from being renamed the FBI—the firefight was a continuation of a busy year of battling gangsters.** In 1934, notorious public enemies like John Dillinger, “Pretty Boy” Floyd, and “Baby Face” Nelson had fallen at the hands of Bureau agents. Heading into 1935, the top priority was to put a dangerous gang—led by the wily Alvin “Creepy” Karpis and a pair of Barker brothers—out of business.

The gang got the Bureau's attention through two high-profile kidnappings. The second targeted a wealthy banker named Edward George Bremer, Jr., who was snatched in St. Paul, Minnesota on January 17, 1934. Bremer was released three weeks later after his family paid \$200,000 in ransom. Although he couldn't identify the culprits, Bremer provided many clues. A key break came when the fingerprint of Arthur “Doc” or “Dock” Barker, a known criminal, turned up on an empty gas can found by a local police officer along the kidnapping route. Soon, a number of Barker's confederates—including his brother Fred, Karpis, Harry Campbell, Fred Goetz, Russell Gibson, Volney Davis, and others—were linked to the crime.

**The hunt was on, but the gang had a head start.** They had split up and begun crisscrossing the country—with some even fleeing to Cuba. Three went as far as to undergo back-room plastic surgeries to conceal their fingerprints and identities. Others passed the ransom loot back and forth and looked for ways to launder the bills.

In late September, Fred Barker and Campbell registered under fake names at the El Comodore Hotel in Miami. Joining them was Fred's mother—Kate “Ma” Barker, who was known to help her criminal sons. When Fred asked for a quiet place to live, the hotel manager told him of a friend's cottage for rent on the nearby Lake Weir. The Barkers moved there in November.

**In December, Doc Barker was tracked by Bureau investigators to a home in Chicago.** On January 8, Doc was arrested without incident. Later that night, several



The Barkers were heavily armed at a cottage near Lake Weir, Florida, where they engaged in a shootout with Bureau agents in 1935. The weapons above were seized following the gunfight.

associates of Russell Gibson were also apprehended. Heavily armed and wearing a bullet-proof vest, Gibson tried to fight it out but was mortally wounded. Searching the apartment, agents found powerful firearms and loads of ammunition. And, tellingly, a map of Florida—with Lake Weir circled. Agents soon located the cottage hideout.

Shortly after 5 a.m. on January 16, 1935, a group of agents led by Earl Connelly surrounded the house and demanded the Barkers' surrender. No response. They waited 15 minutes and called again. Again, no answer. Following another call for surrender and more silence, agents shot some tear gas grenades at the windows of the house. Someone in the house shouted, “All right, go ahead,” then machine-gun fire blasted from the upstairs window.

The agents responded with volleys of their own; more gunfire erupted from the house. Over the next hour, intermittent shots came from the home, and agents returned fire. By 10:30 a.m., all firing had stopped. Both Ma and Fred, it was soon learned, were dead.

**The Barkers were history, but the cunning Karpis was still on the loose.** How we caught up with him is another story that we'll tell in the coming months.





## Cargo Theft

### How a Memphis Task Force Combats a Costly Problem

After many hours on the road, the long-haul driver pulled his tractor-trailer into a Tennessee truck stop for a break and a hot meal. But by the time he looked over the menu, a crew of professional thieves had made off with his rig and all its contents.

**Cargo theft is a multi-billion-dollar criminal enterprise in the U.S., and the FBI has seven task forces located around the country to combat the problem.** In the Memphis region, according to Special Agent Conrad Straube, coordinator of the Memphis Cargo Theft Task Force, “there is an average of one cargo theft every day of the year.”

Memphis—located along major interstate highways and home to a variety of product distribution centers—is a hot spot for cargo theft. The thieves steal trucks with trailers or just the trailers and their contents. Often, goods are stolen from distribution center warehouses or even from moving rail cars.

On a recent day, Straube and his task force partners from the Memphis Police Department, the Shelby County Sheriff’s Office, and the U.S. Marshals Service were on the road, following up on leads at truck stops and other locations in and around Memphis. The task force is busy—and successful. From January 2011 to the end of September, it recovered more than \$1.5 million in stolen cargo and vehicles.

Task force member Barry Clark, a detective with the Shelby County Sheriff’s Office, explained that some of the theft crews are so organized that each member has his

own specialty, from the break-in artist who can steal a rig in seconds to professional drivers, surveillance experts, and the guys who know how to defeat the specialized devices that lock trailers carrying extremely valuable loads. “This is their business,” Clark said. “And they are good at it.”

Crew leaders know where to find willing buyers, too—from small mom and pop stores who don’t ask questions when they buy at prices below wholesale to online merchants who may or may not know they are purchasing stolen goods.

Although many crews target specific cargo such as electronics and pharmaceuticals—always in demand and easy to sell—other thieves steal whatever they can get their hands on. Straube and his team have recovered stolen trailers full of dog food, hair dryers, lawn mower engines, and even Popsicles.

**“When you talk about the victims of cargo theft,” Straube explained, “beyond the trucking companies and manufacturers, you have to include all consumers. Because when these items are stolen, it eventually drives up the cost of merchandise for everybody.”**

Cargo theft is also a “gateway” crime, said Special Agent Eric Ives, a program manager in our Criminal Investigative Division at FBI Headquarters who coordinates major theft investigations from a national perspective. “Groups that do these crimes are often funding other illegal activities, like buying drugs or weapons. And compared to many crimes,” Ives added, “cargo theft is highly profitable and not particularly dangerous.”

Conrad agreed, adding that thieves often rob warehouses on a Friday night, and by the time the crime is discovered and reported Monday morning, the stolen merchandise may already be on a store shelf or auctioned online.

That’s why our task forces—comprised of local, state, and federal law enforcement—and our partnerships with private industry are critical in the fight against these costly crimes, Ives said. “Cargo theft is a sophisticated and organized enterprise,” he added, “and we take this threat very seriously.”



Scan this QR code with your smartphone to watch a related video, or visit <http://www.fbi.gov/news/videos/>.

# Investigating Insurance Fraud

## A \$30-Billion-a-Year Racket

Putting the brakes on major white-collar frauds of all kinds is one of our most important responsibilities, and there is no shortage of work these days for the FBI and its partners.

Our corporate and securities fraud cases, for example, resulted in more than 600 convictions last year—including a number of high-level executives—and more than \$23 billion in recoveries, fines, and restitutions over the past three years. Our mortgage fraud efforts continue to pinpoint the most egregious offenders; approximately 70 percent of our 3,000 pending mortgage fraud investigations involve losses of more than \$1 million. There are also plenty of cases involving health care fraud, bankruptcy fraud, credit card fraud, mass marketing fraud, and various wire and mail fraud schemes.

**Insurance fraud—non-health care-related fraud involving casualty, property, disability, and life insurance—is another financial crime that falls under FBI jurisdiction.** The U.S. insurance industry consists of thousands of companies that collect more than \$1.1 trillion in premiums each year, according to the Insurance Information Institute, and the estimated cost of fraud is approximately \$30 billion a year. Most of this expense is passed on to consumers in the form of higher insurance premiums, to the tune of about \$200 to \$300 a year per family, according to the National Insurance Crime Bureau. Not to mention the number of insurance companies that go under because of excessive claims and/or the looting of company assets.

There are many capable private and government investigative and regulatory entities at the national and state level that look into insurance fraud, so the FBI directs its resources toward identifying the most prevalent schemes and the top-echelon criminals and criminal organizations who commit the fraud. But even when conducting our own investigations, we often work closely with private fraud associations, state fraud bureaus, state insurance regulators, and other federal agencies.

**The FBI currently focuses on the following schemes:**

- Disaster-related fraud, which became such a problem after Hurricane Katrina that a special task force was created to address it (and evolved into today's National Center for Disaster Fraud);



- Premium and asset diversion, which happens when insurance agents, brokers, and even insurance company executives steal insurance premiums submitted by policyholders and sometimes plunder company financial assets for their own personal use;
- Viatical fraud (a “viatical” settlement is one where an investor buys the right to receive the benefit of a terminally ill or elderly person’s life insurance policy);
- Staged auto accidents;
- Bodily injury fraud; and
- Property insurance fraud.

**Who commits insurance fraud?** In most cases it’s dishonest policyholders, insurance industry insiders (i.e., agents, brokers, company execs), and loosely organized networks of crooked medical professionals and attorneys who use their knowledge to bypass anti-fraud measures put in place by insurance companies.

**How we investigate it.** Like many other white-collar crime investigations, insurance fraud is mostly about following the money trail—which often involves questioning victims and victim companies, reviewing financial documents, and using sensitive techniques like sources and cooperating witnesses.

We also use our intelligence capabilities to keep our finger on the pulse of emerging trends—for example, as more insurance companies conduct business online, we fully expect to see a rise in the theft of policyholders’ identities and in cyber-based insurance scams. We will keep you posted.





## Protecting Civil Rights

### Part 1: Memphis Agent Seeks Justice for Victims

Special Agent Tracey Harris is a 13-year veteran of the FBI who specializes in civil rights cases such as hate crimes and human trafficking. But it's not just her job—it's her passion.

When she transferred back to her native Memphis, Tennessee in 2003 and landed on the civil rights squad, it was not her top choice—that is, until her first case, which involved a police officer who raped a 12-year-old girl in his squad car while he was on duty.

**"That's when I realized that somebody has to do these cases," Harris said.** "Many civil rights victims represent the social ills of the world," she explained. "They may be prostitutes, victims of human trafficking, or individuals abused by police. These are not generally people who have strong family ties or come from stable homes. They often have no voice. It's our job," Harris said, "to give them a voice. Somebody has to speak for these victims."

Harris works closely with the agents on her squad and with the U.S. Attorney's Office for the Western District of Tennessee, which is one of the nation's leading prosecutors of federal civil rights cases.

**"This community has a legacy of being on the front lines of civil rights issues,"** said Edward Stanton, III, U.S. Attorney for the Western District of Tennessee. In February 2011, Stanton established a dedicated civil rights unit and announced the initiative at the National Civil Rights Museum in Memphis, located on the site where the Rev. Martin Luther King, Jr. was slain.

"I don't think it's by happenstance or coincidence that our district often leads the nation in civil rights prosecutions," Stanton said. "We couldn't do that without our partners from the FBI. At the end of the day, pursuing justice remains the bottom-line goal for both agencies. Our prosecutors and their FBI colleagues have a special bond and a dedication to these cases."

**That special bond is due in part to the unique nature of civil rights cases, said Assistant United States Attorney Steve Parker, who heads the civil rights unit in Memphis.**

In many federal criminal investigations, agents bring a fully investigated case to a prosecutor for trial. Civil rights cases are different, Parker said, because they rely more on grand juries to gather information. "Witnesses in civil rights cases don't come forward on their own because they are usually close associates or friends of the defendants," he explained. "It takes the leverage of the grand jury and the expertise of the investigators and prosecutors working together to successfully deal with these cases."

Parker added, "I work 90 percent cases of my cases with the FBI's civil rights squad. We do interviews together and go to grand juries together—we work together very closely just about every day."

Agent Harris acknowledged that civil rights cases can be emotionally difficult and can take years to resolve. "You deal with that by taking them one case at a time and one prosecution at a time," she said. "And you are gratified when the bad guys go to jail and the victims and their families get some measure of justice."

One such difficult case that Harris and prosecutors are especially proud of involved the murder of a 46-year-old Memphis code enforcement officer and father of five named Mickey Wright. His killer, Harris said, "took Mickey's life just because he was black."

*Part 2: Bringing Mickey Wright's murderer to justice (page 11)*

# Protecting Civil Rights

## Part 2: Closing a Memphis Murder Case

Mickey Wright, a 46-year-old devoted father of five, was a code enforcement officer for the city of Memphis, Tennessee. “One day he went to work,” said Special Agent Tracey Harris, “and he never came home.”

**During a routine stop at an auto repair business in 2001, Wright was murdered—“just because he was black,” Harris said.**

The Mickey Wright case outraged the Memphis community and illustrates not only how emotionally charged civil rights cases can be, said Harris, but how difficult they are to investigate and prosecute.

Wright went missing on April 17, 2001. Two days later, his work identification badge and other personal items were found in a ditch about 20 miles outside of Memphis. Ten days after his disappearance, Wright’s burned code enforcement truck was discovered in a Mississippi field.

Suspicion fell on Dale Mardis, a gun dealer who owned the property where the auto repair shop was located. But it would be three years after the killing before Mardis was charged by the state of Tennessee with second-degree murder. In 2007, he was allowed to plead no contest—acknowledging that the state had enough evidence to convict him but not having to admit guilt in the murder. He began serving a 15-year sentence.

“This was a very public case,” Harris said, “and there was a public outcry when Mardis entered his plea and only got 15 years. Mickey Wright’s body was still missing, and many believed this was a hate crime—a far more serious offense than the second-degree murder charge.”

On behalf of Wright’s family, a local official asked the FBI to investigate the case as a civil rights matter. With Mardis in jail, some of the witnesses who had earlier perjured themselves during the state proceedings felt more comfortable telling the truth, Harris said. “And we located new witnesses whom Mardis had told about the crime.”

**In 2008, federal prosecutors charged Mardis with the racially motivated killing of Wright.** That April day when Wright stopped at the auto repair shop, Mardis became incensed and shot him. Federal prosecutors said Mardis often fought with code enforcement inspectors, especially if they were black. Mardis later admitted to burning the body with diesel fuel in a 55-gallon drum.



**Two days after Mickey Wright went missing in 2001, his work identification badge and other personal items were found in a ditch about 20 miles outside of Memphis.**

During the FBI investigation, Harris said, a witness also implicated Mardis in another murder, to which he also pled guilty. Last July, 10 years after Mickey Wright’s murder, Mardis was sentenced to life in prison without the possibility of parole—and he finally admitted publicly to the hate crime he committed.

“It really meant a lot when we were able to get that guilty plea and life sentence,” said Assistant United States Attorney Jonathan Skrmetti, who prosecuted the case. “Mickey Wright’s family was there with us in the courtroom, and we were able to explain to them that this man would never again be out on the streets.”

“This case was personally very rewarding,” Harris added, “but more importantly, it was good for the community. People were angered by this case, and—together with the U.S. Attorney’s Office—we helped restore the public’s faith in the criminal justice system. That’s a very good feeling.”



Scan this QR code with your smartphone to watch a related video, or visit <http://www.fbi.gov/news/videos/>.





## Cyber Alerts for Parents & Kids

### Tip #2: Beware of 'Sextortion'

At the beginning of her summer break in June 2005, a 15-year-old Florida girl logged onto her computer and received a startling instant message. The sender, whom the girl didn't know, said he had seen her photo online and that he wanted her to send him pictures—of her in the shower. When the girl didn't comply, the sender showed he knew where she lived and threatened to hurt the girl's sister if she didn't agree to his demands.

Worried and hoping to avoid alarming her parents, the girl sent 10 black-and-white images. When her harasser said they weren't good enough, she sent 10 more, nude and in color. Then he wanted more.

**"Once these individuals have pictures, they want more,"** said Special Agent Nickolas B. Savage, who interviewed the girl after she and her mother contacted authorities. "They are then able to say, 'I want you to do x, y, and z. And if you don't, I'm going to take these photographs and I'm going to send them to people in your school. I'll send them to your family.'"

Savage, who at the time managed the Innocent Images National Initiative Task Force in the FBI's Orlando office, spent the better part of the next four years chasing the phantoms that had hacked the 15-year-old's computer. The winding path eventually led to two assailants—Patrick Connolly and Ivory Dickerson—who jointly terrorized adolescent girls by compromising their computers, demanding sexual photos or videos, and scouring their social networks. The pair also reached out to the girls' friends—who were duped into downloading malicious

software because the e-mails and messages appeared to come from trusted sources.

**Connolly and Dickerson, both in prison now, victimized more than 3,800 kids through this "sextortion" technique that preyed on kids' innocence about the Internet and their fear of being exposed to their friends and family.**

"Oftentimes children are embarrassed, especially thinking they have somehow contributed to their victimization," said Savage, who now helps lead the Strategic Outreach and Initiative Section in the Cyber Division. "So fearing they will get in trouble if they report it, they will continue with the victimization and send individuals what they are requesting. What often happens is the victimization never stops."

**In this case, some girls were terrorized over a span of as many as seven years.** Some attempted suicide. One dropped out of high school because she was always looking over her shoulder.

To uncover the scheme, the FBI cloned one of the victim's computers and carried on a two-year undercover correspondence with the hacker, who turned out to be Connolly—a British citizen who was at times in Saudi Arabia and Iraq, where he worked as a military contractor and evidently carried out parts of his extortion scheme. The trail also led to North Carolina, where Dickerson was amassing a huge portfolio of pictures and videos and secretly recording the webcams of compromised computers. Dickerson was found to have about 230 gigabytes of material; Connolly had four times that. Dickerson was sentenced in 2007 to 110 years in prison. Three years later, Connolly was sentenced to 30 years.

Savage says locking up the hackers was one of the most rewarding moments in his career. But he knows there are more victims, some who may not know their tormentors are off the streets.

"The thing was, a lot of these kids are just some folder somewhere," Savage said, illustrating the cold nature of the crimes and punctuating that once material is posted online, it's out there for all to see. "No name. Just pictures and videos in a folder. I know that there are so many more victims out there that are wondering, 'What ever happened to those guys?' or, 'Do I still need to be afraid?'"

*This story is the second in an occasional series aimed at providing practical web advice and tips for parents and their kids. For tip #1, visit [www.fbi.gov/news/stories/2011/december/cyber\\_122211](http://www.fbi.gov/news/stories/2011/december/cyber_122211).*

## Looking for Love?

### Beware of Online Dating Scams

Millions of Americans visit online dating websites every year hoping to find a companion or even a soul mate.

But today, on Valentine's Day, we want to warn you that criminals use these sites, too, looking to turn the lonely and vulnerable into fast money through a variety of scams.

These criminals—who also troll social media sites and chat rooms in search of romantic victims—usually claim to be Americans traveling or working abroad. In reality, they often live overseas. Their most common targets are women over 40 who are divorced, widowed, and/or disabled, but every age group and demographic is at risk.

**Here's how the scam usually works.** You're contacted online by someone who appears interested in you. He or she may have a profile you can read or a picture that is e-mailed to you. For weeks, even months, you may chat back and forth with one another, forming a connection. You may even be sent flowers or other gifts. But ultimately, it's going to happen—your new-found “friend” is going to ask you for money.

#### Recognizing an Online Dating Scam Artist

Your online “date” may only be interested in your money if he or she:

- Presses you to leave the dating website you met through and to communicate using personal e-mail or instant messaging;
- Professes instant feelings of love;
- Sends you a photograph of himself or herself that looks like something from a glamour magazine;
- Claims to be from the U.S. and is traveling or working overseas;
- Makes plans to visit you but is then unable to do so because of a tragic event; or
- Asks for money for a variety of reasons (travel, medical emergencies, hotel bills, hospitals bills for a child or other relative, visas or other official documents, losses from a financial setback or crime victimization).

One way to steer clear of these criminals all together is to stick to online dating websites with nationally known reputations.

So you send money...but rest assured the requests won't stop there. There will be more hardships that only you can help alleviate with your financial gifts. He may also send you checks to cash since he's out of the country and can't cash them himself, or he may ask you to forward him a package.



**So what really happened?** You were targeted by criminals, probably based on personal information you uploaded on dating or social media sites. The pictures you were sent were most likely phony, lifted from other websites. The profiles were fake as well, carefully crafted to match your interests.

In addition to losing your money to someone who had no intention of ever visiting you, you may also have unknowingly taken part in a money laundering scheme by cashing phony checks and sending the money overseas and by shipping stolen merchandise (the forwarded package).

While the FBI and other federal partners work some of these cases—in particular those with a large number of victims or large dollar losses and/or those involving organized criminal groups—many are investigated by local and state authorities.

**We strongly recommend, however, that if you think you've been victimized by a dating scam or any other online scam, file a complaint with our Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov).** Before forwarding the complaints to the appropriate agencies, IC3 collates and analyzes the data—looking for common threads that could link complaints together and help identify the culprits. Which helps keep everyone safer on the Internet.

For specific tips on how to keep from being lured into an online dating scam, see the sidebar (left). Awareness is the best tool for preventing crime...and in this case, even for preventing a broken heart.





## Trying to Sell That Timeshare?

### Beware of Fraudsters

Last October, after a joint FBI-Ft. Lauderdale Police Department investigation, 13 individuals from a Florida timeshare resale company were charged in federal court in Miami for their roles in a massive telemarketing scheme to defraud timeshare owners who were trying to sell. The Federal Trade Commission then filed a complaint against the defendants' company—Timeshare Mega Media—to shut down its operations, which had allegedly bilked millions from owners across the country.

**Fraudulent timeshare schemes are becoming a very real problem...**...especially in these economically challenging times as more timeshare owners decide they can no longer afford them. A timeshare involves joint ownership of a property—usually located within resorts in vacation hotspots (i.e., Florida, Colorado, Mexico). A property can have up to 52 owners—one for each week of the year—although some timeshare owners purchase larger blocks of time. The property is usually managed by the resort in which it is located.

**Earlier this year, the FBI's Internet Crime Complaint Center (IC3) issued an alert on timeshare telemarketing scams after seeing a significant increase in the number of complaints about these scams.** The victims—mostly owners trying to sell—were scammed by criminals posing as representatives of timeshare resale companies or by actual employees of companies that were committing fraud.

In the IC3 complaints, perpetrators telephoned or e-mailed timeshare owners who, in many instances, had advertised their desire to sell in industry newsletters and

websites. These company representatives promised a quick sale, often within 60-90 days. Some victims reported that sales reps pressured them into a quick decision by claiming there was a buyer waiting in the wings, either on the other line or in the office. Timeshare owners who agreed to sell had to pay an upfront fee—anywhere from a few hundred to a few thousand dollars—to cover various costs such as advertising or closing fees. Many victims provided credit card numbers to cover the fees.

And then, as time went on and no sales were made, victims tried reaching back out to the companies, but their phone calls and e-mails went unanswered.

And to add insult to injury, some of the complainants reported being contacted by a timeshare fraud recovery company that promised assistance in recovering money lost in the sales scam...for a fee. IC3 has identified some instances where people involved with the recovery company have a connection to the resale company, raising the possibility that victims were being scammed twice by the same people.

**What's the FBI's role in these kinds of cases?** Many of these types of complaints are handled by each state's attorney general's office and local law enforcement. As in the above-mentioned Miami case, the FBI can become involved when there's evidence that the fraud extends across state lines (usually wire or mail fraud on the part of the perpetrators) and/or involves a large number of victims, large dollar losses, and an organized criminal enterprise.

**If you suspect you've been scammed, file a complaint with your state attorney general's office and the IC3 ([www.ic3.gov](http://www.ic3.gov)).** The IC3 not only collects complaints but also analyzes them, links similar complaints, and discerns patterns in order to help law enforcement identify the scammers.

# On Guard Against WMD

## Inside the Biological Countermeasures Unit, Part 1

In 2006, to counter the threat posed by weapons of mass destruction (WMD), the FBI established the WMD Directorate. The directorate combines law enforcement investigative authorities, intelligence analysis capabilities, and technical subject matter expertise in a coordinated approach to deal with incidents involving nuclear, radiological, biological, or chemical weapons. The organization places substantial emphasis on preventing such incidents.

FBI.gov recently spoke with Special Agent Edward You in the directorate's Biological Countermeasures Unit (BCU).

### **Q: What is your unit's primary mission?**

**Mr. You:** Just like our partner units who also work in countermeasures dealing with chemicals, radiological and nuclear material, and infrastructure protection, our goal is to prevent acts of terrorism. In our case, that means bio-terrorism. But we must do that in a way that strikes a balance between security and supporting advances in scientific research and protecting public safety. Bio-security, from our standpoint, is preventing the illicit acquisition or misuse of the technologies, practices, and materials associated with biological sciences. We are also charged with protecting scientists and the institutions where they work.

### **Q: What are the primary biological WMD risks?**

**Mr. You:** Laboratory techniques for biological materials are publicly available in scientific journals and elsewhere, which represent a ready source of knowledge for creating and manipulating these materials. Biological agents such as viruses, bacteria, and toxins are also widely available and used in companies, universities, and other institutions. These include materials that could have devastating effects on the public if released, such as avian influenza or *Bacillus anthracis* spores (anthrax). These things are also naturally occurring in the environment. Both the methods and the materials are critical for scientific research and the development of beneficial products. But we also recognize that the materials could be exploited or subverted for terrorist or criminal acts. We conduct outreach to try to make people aware of these risks.

### **Q: How important are partnerships between law enforcement and the medical and scientific community?**



**Mr. You:** They are essential. We have a joint criminal-epidemiological investigation model, which is how law enforcement works together with public health entities to quickly assess an unusual disease outbreak to determine if it is naturally occurring or was started intentionally. The partnership is critical to ensure rapid sharing of information to guide the appropriate investigative steps and responses. All these efforts address the shared goal of protecting public health and safety—again, without hindering scientific progress.

### **Q: What is your primary means of conducting outreach?**

**Mr. You:** We provide opportunities for the scientific community to meet directly with our law enforcement representatives—our WMD coordinators. These are the FBI's subject matter experts, local points of contact, and really the keystone of the entire program. Each of our 56 field offices nationwide has at least one of these special agent coordinators trained in the various WMD modalities. They are the focal point for state and local law enforcement and public health officials. Coordinators conduct outreach and liaison development with academia, institutions, industry contacts, and other organizations. Our unit at FBI Headquarters manages the outreach program at the national level. We facilitate meetings between our coordinators and members of the biological sciences community, provide a mutual understanding of bio-security from a law enforcement perspective, and foster partnerships nationwide. We are also branching out internationally, with WMD personnel in Eastern Europe, Singapore, and at INTERPOL in France.

*Part 2: Training, tripwires, and more (page 16)*



## On Guard Against WMD

### Inside the Biological Countermeasures Unit, Part 2

*Part 2 of an interview with Special Agent Edward You of the Biological Countermeasures Unit in the Weapons of Mass Destruction (WMD) Directorate.*

**Q: What other responsibilities do WMD coordinators have?**

**Mr. You:** At the local level, WMD coordinators act as resources for our partners and they also engage in threat assessments and investigations. Coordinators are dedicated professionals who have their own career path within the FBI and they go through an extensive training and certification program. With regard to training, we have partnered with the Centers for Disease Control and Prevention to provide training locally, regionally, and internationally. We are able to educate the scientific community about threats and provide situational awareness about security issues that may not have been considered. In turn, the scientific community advises law enforcement about the current state of the field and assists us in identifying over-the-horizon risks. The life sciences field is advancing so rapidly that it is difficult to stay current. We rely on the expertise of our business and academic partners to ensure that our agency is addressing issues appropriately and effectively. Synthetic biology is a case in point.

**Q: What is synthetic biology?**

**Mr. You:** It is the application of engineering and computer science principles to the life sciences. It is an evolutionary step in techniques in DNA sequencing and synthesis that are used to modify naturally occurring

organisms, such as yeast and bacteria, and “reprogram” them to impart novel functions not normally found in nature. For example, synthetic biology allows you to program bacteria to efficiently produce bio-diesel fuel, medicines, and building materials.

**Q: Why is synthetic biology important in terms of WMD?**

**Mr. You:** Consider a company that produces synthetic DNA. They have the ability to generate the necessary genetic information to potentially produce bacteria and viruses, even high-consequence biological agents—such as Ebola or *Bacillus anthracis* (anthrax)—that are regulated by the U.S. government. Companies have adopted screening measures to prevent uncertified individuals from purchasing genetic information for these high-consequence agents.

Through our outreach efforts and subsequent federal guidance, companies now know to contact our WMD coordinators when they encounter suspicious orders. The FBI can conduct further assessments, provide information back to the companies, and initiate investigations if warranted. As a result, industry was very happy to have a vehicle for reporting and vetting suspicious activity. We really filled a need with this program, and it has been very successful.

**Q: How will you continue to be successful going forward?**

**Mr. You:** We will continue working with industry and the scientific community. Because we provide a service and act as a resource for our partners, our outreach has grown at a rapid pace—we can’t keep up with demand in terms of speaking engagements we are invited to or contributions to biosecurity policymaking. When we started our outreach program five years ago, we were out knocking on doors in the scientific community, trying to spread our message. Now they are inviting us in. They obviously they see the value of what we’re doing to protect the public and the scientific process.



# The State of Financial Crime

## Our Latest Accounting

The founder of a \$7 billion hedge fund is convicted of insider trading. A drug company pleads guilty to making and selling unsafe prescription drugs to Americans. The head of a financial company admits scamming distressed homeowners who were trying to avoid foreclosure.

These recent crimes and many more like them—investigated by the FBI, in some instances along with our partner agencies—can cause great harm to the U.S. economy and American consumers. That's why financial crimes are such an investigative priority at the Bureau.

Today, we're releasing an overview of the problem and our response to it in our latest *Financial Crimes Report to the Public*. The report—which covers the period from October 1, 2009, to September 30, 2011—explains dozens of fraud schemes, outlines emerging trends, details FBI accomplishments in combating financial crimes (including major cases), and offers tips on protecting yourself from these crimes.

### Here's a brief snapshot of key sections of the report:

**Corporate fraud:** One of the Bureau's highest criminal priorities, our corporate fraud cases resulted in 242 indictments/informations and 241 convictions of corporate criminals during fiscal year (FY) 2011. While most of our cases involve accounting schemes designed to conceal the true condition of a corporation or business, we've seen an increase in the number of insider trading cases.

**Securities/commodities fraud:** In FY 2011, our cases resulted in 520 indictments/informations and 394 convictions. As a result of an often volatile market, we've seen a rise in this type of fraud as investors look for alternative investment opportunities. There have been increases in new scams—like securities market manipulation via cyber intrusion—as well as the tried-and-true—like Ponzi schemes.

**Health care fraud:** In FY 2011, 2,690 cases investigated by the FBI resulted in 1,676 informations/indictments and 736 convictions. Some of the more prevalent schemes included billing for services not provided, duplicate claims, medically unnecessary services, upcoding of services or equipment, and kickbacks for referring patients for services paid for by Medicare/Medicaid. We've seen increasing involvement of organized criminal groups in many of these schemes.



In a public service announcement for the FBI, actor Michael Douglas, who played a financial executive in the movie *Wall Street*, says that while the 1987 movie was fiction, the problem is all too real.

**Mortgage fraud:** During 2011, mortgage origination loans were at their lowest levels since 2001, partially due to tighter underwriting standards, while foreclosures and delinquencies have skyrocketed over the past few years. So, distressed homeowner fraud has replaced loan origination fraud as the number one mortgage fraud threat in many FBI offices. Other schemes include illegal property flipping, equity skimming, loan modification schemes, and builder bailout/condo conversion. During FY 2011, we had 2,691 pending mortgage fraud cases.

**Financial institution fraud:** Investigations in this area focused on insider fraud (embezzlement and misapplication), check fraud, counterfeit negotiable instruments, check kiting, and fraud contributing to the failure of financial institutions. The FBI has been especially busy with that last one—in FY 2010, 157 banks failed, the highest number since 181 financial institutions closed in 1992 at the height of the savings and loan crisis.

Also mentioned in the report are two recent initiatives that support our efforts against financial crime: the **forensic accountant program**, which ensures that financial investigative matters are conducted with the high-level expertise needed in an increasingly complex global financial system; and our **Financial Intelligence Center**, which provides tactical analysis of financial intelligence data, identifies potential criminal enterprises, and enhances investigations. More on these initiatives in the future.



Scan this QR code with your smartphone to watch the public service announcement featuring Michael Douglas, or visit <http://www.fbi.gov/news/videos/>.



## Operation Atlantic

### Taking International Aim at Child Predators

On Wednesday, Europol released the results of its first joint operation with the FBI against international child predators, announcing the identification of eight child victims and the arrest of 17 individuals for child sexual molestation and production of pornography.

**Operation Atlantic has led to the identification of 37 child sex offenders in France, Italy, the Netherlands, Spain, and the United Kingdom.** The investigation, which began in December 2010, continues as individuals overseas are still being sought.

“Online child predators and child exploitation are not just an American problem,” said FBI Director Robert S. Mueller. “The FBI is committed to working with our law enforcement partners around the world, such as Europol, to combat these horrendous crimes. We share actionable intelligence and resources to keep children safe and bring those who do them harm to justice.”

Sharing intelligence was our primary role in Operation Atlantic, and it was facilitated by our Innocent Images Operations Unit (IIOU) at FBI Headquarters. Agents working covertly set up an electronic dragnet on a peer-to-peer network targeting pedophiles located in European Union (EU) countries and forwarded investigative results to our partners at Europol.

Previously, IIOU staff worked with our legal attachés overseas to formalize a cooperative agreement with Europol regarding several criminal investigative programs, including online child sexual exploitation. “The results of Operation Atlantic validate this new relationship and

offer an example of outstanding achievement through international law enforcement cooperation,” said Audrey McNeill, IIOU chief.

Europol works with law enforcement agencies in the 27 EU countries, along with non-EU members such as the U.S. and Australia. Europol personnel do not have direct powers of arrest, but instead support law enforcement in member countries through coordination and intelligence gathering and sharing.

**“Collaboration and cooperation between Europol and our international law enforcement partners such as the FBI are essential if we are to bring members of these child sex abuse networks to justice and prevent the distribution of child exploitation material across the Internet,”** said Rob Wainwright, Europol’s director. Noting that Operation Atlantic is the first joint operation conducted by the FBI and Europol in the area of child sexual exploitation, Wainwright added, “Europol is ready and willing to support ongoing and future operations to infiltrate these networks.”

The leads and intelligence gathered by the FBI that formed the basis of Operation Atlantic helped link suspects in five countries to pedophile groups, including the notorious “Boylover” network—the focus of a previous Europol action called Operation Rescue. Subjects arrested in Operation Atlantic included a web of offenders that were producing and distributing images depicting the severe abuse of children—in some cases toddlers and infants.

“These individuals were not just possessors of child pornography,” McNeill said. “Some were previously convicted child sex offenders and were actively engaged in child sexual abuse.” In addition to providing leads to Europol, the IIOU detailed an agent to Europol headquarters in The Hague, Netherlands last summer to help facilitate the investigation.

“Europol is a key and valued strategic partner for the IIOU, and we look forward to a long and productive relationship with them,” McNeill said. “I hope that Operation Atlantic is the first of many future successes. We are working hard to increase our international footprint and to stop child predators wherever they are in the world.”

# Help Us Bring Bob Levinson Home

## \$1 Million Reward Offered for Missing Retired FBI Agent

This week marks the fifth anniversary of Robert Levinson's disappearance, and the FBI today announced a reward of up to \$1 million for information leading to the safe recovery and return of the retired special agent.

Levinson, who retired from the FBI in 1998 after 22 years of service, was working as a private investigator when he traveled to Kish Island, Iran on March 8, 2007. He has not been seen or heard from publicly since he disappeared the following day. In 2010, a video showing him in captivity was sent to the Levinson family by his captors.

**The FBI is responsible for investigating crimes committed against U.S. citizens abroad. We have been working since 2007 to obtain information about Levinson's whereabouts and well-being.**

"On the fifth anniversary of Bob's disappearance, the FBI continues to follow every lead into his abduction and captivity," said James W. McJunkin, assistant director in charge of our Washington Field Office. "We are committed to bringing Bob home safely to his family. We hope this reward will encourage anyone with information—no matter how insignificant they may think it is—to come forward. It may be the clue that we need to locate Bob."

"Though he is retired from the FBI, Bob remains a member of the FBI family to this day," said Director Robert S. Mueller, "and his family is our family. Like all families, we stand together in good times and in times of adversity. Today, we stand together to reaffirm our commitment to Bob Levinson."

"I am very grateful that the FBI has offered this reward," said Levinson's wife Christine. "Our family believes the only way of resolving this issue successfully is with the FBI's help. It has been an extremely difficult time for my family," she said. "We all thought Bob would be home by now. But five years have passed, and we still don't know why he's being held, who has him, or where he is."

**Levinson will celebrate his 64th birthday on March 10.** In addition to his wife of 37 years, Levinson has seven children and two grandchildren. The family has been working tirelessly to bring Levinson home safely. "Our youngest son is about to graduate from high school,"



Robert Levinson, a retired FBI agent, went missing from Kish Island, Iran on March 8, 2007.

Christine Levinson said. "He was in middle school when his father disappeared."

In March 2011, the U.S. secretary of state issued a statement that the U.S. government had received indications that Levinson was being held by a group in southwest Asia. That region includes the border areas of Afghanistan, Iran, and Pakistan. A publicity campaign is being launched this week in southwest Asia to heighten awareness of Levinson's abduction, announce the \$1,000,000 reward, and solicit information. Billboards, radio messages, and flyers will be used to publicize the reward and the investigation. A telephone tip line will be provided to listeners and viewers in that region so that they can confidentially provide information.

"We're never going to give up," Christine Levinson said. "Our goal is to get Bob home. We miss him every single day."

**We need your help.** If you have information about the Levinson case, contact your nearest FBI office or American Embassy, or submit a tip to <https://tips.fbi.gov>.



Scan this QR code with your smartphone to watch a video released by the Levinson family, or visit <http://www.fbi.gov/news/videos/>.





## FBI Forensic Accountants

### Following the Money

Accountants have been woven into the fabric of the FBI since its creation in the summer of 1908, when a dozen bank examiners were included among the original force of 34 investigators. Today, around 15 percent of agents employed by the Bureau qualify as special agent accountants.

Non-agent accounting positions at the FBI date back to the early 1970s, when we created a cadre of accounting technicians to help agents working increasingly complex financial cases. During the savings and loan crisis of the 1980s and 1990s, the FBI's ability to address complex, sophisticated financial investigations was elevated further with the addition of financial analysts to our ranks.

Post-9/11, the criminal landscape changed again with large-scale corporate frauds and a multitude of other complex financial schemes. And once again, we adapted by adding new resources and skills. One key element was the 2009 creation of a standardized, professional investigative support position known as a forensic accountant.

**At the FBI, our forensic accountants conduct the financial investigative portion of complex cases across a wide variety of Bureau programs—investigating terrorists, spies, and criminals of all kinds who are involved in financial wrongdoing.** Through their work, forensic accountants contribute to the FBI's intelligence cycle. They testify to their findings in court. And they keep up to date with FBI policies and procedures, federal rules of evidence, grand jury procedures, and national security protocols.

#### Responsibilities of FBI forensic accountants include:

- Conducting thorough forensic financial analysis of business and personal records and developing financial profiles of individuals or groups identified as participating in suspicious or illegal activity;
- Participating in gathering evidence and preparing search warrants/affidavits associated with financial analysis;
- Accompanying case agents on interviews of subjects and key witnesses in secure and non-confrontational settings;
- Identifying and tracing funding sources and inter-related transactions;
- Compiling findings and conclusions into financial investigative reports; and
- Meeting with prosecuting attorneys to discuss strategies and other litigation support functions and testifying when needed as fact or expert witnesses in judicial proceedings.

**FBI-centric training.** On top of the extensive accounting qualifications they bring to the job, FBI forensic accountants take a six-week training course that focuses on Bureau programs and systems, available investigative resources, financial investigative topics and techniques, legal training, and expert witness testifying techniques.

Forensic accountants are located in every FBI field office. Larger offices might have one or more forensic accountant squads composed of both forensic accountants and financial analysts, while smaller offices might just have one or two forensic accountants. Then there's our Forensic Accountant Support Team (think SWAT for accountants), based out of our Washington, D.C. Headquarters, that responds quickly—either in person or often electronically—to significant, high-profile investigations anywhere in the country involving large amounts of financial data.

FBI forensic accountants have been involved in a number of major cases over the past couple of years, including a \$200 million Medicare fraud case involving two Florida corporations, the largest hedge fund insider trading scheme in history, and a \$200 million fraud by executives of an Indiana financial company.

If you're interested in a career as an FBI forensic accountant, check the [www.fbijobs.gov](http://www.fbijobs.gov) website periodically for open positions.

# Investigating Financial Crime

## A Retrospective

Charles Bonaparte was clearly onto something.

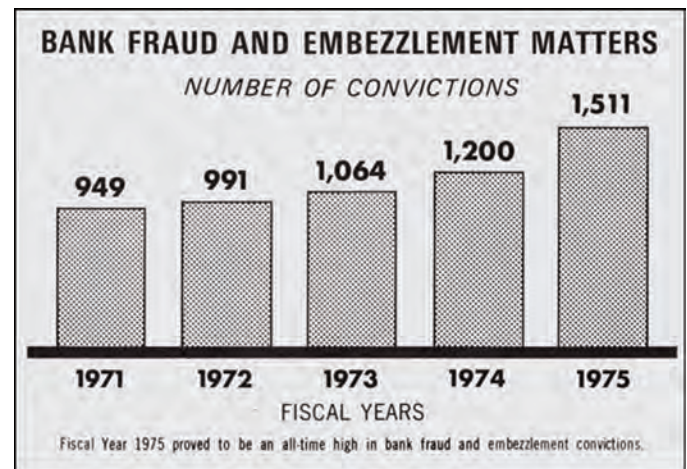
When he created a “special agent force” in 1908—the forerunner of the FBI—the progressive attorney general made sure that a dozen of his first 34 investigators were bank examiners specializing in financial crimes. No doubt to the satisfaction of the muckrakers of the day and his own trust-busting boss, President Teddy Roosevelt.

These experienced financial agents hit the ground running, investigating antitrust activities (now part of our public corruption program) in the meat processing and sardine canning industries. They also tackled a variety of financial frauds—from bankruptcy scams to accounting frauds in federal prisons and courts. The Bureau was also responsible for investigating several national banking law violations.

**Over our first six or seven decades, the financial crimes we investigated were fairly small potatoes by today’s standards.** There were plenty of them, to be sure. Like the “Lady with the Big Heart” who embezzled some \$150,000 from her bank in Trenton, New Jersey in the 1940s and used the stolen loot to pick up dinner tabs and buy expensive gifts for herself and her friends. Like the New York City music producer who convinced an investor to give him \$35,000 in 1942 to finance a *Nutcracker* ballet movie, only to pocket the money and file for bankruptcy. And like Frank Abagnale of *Catch Me If You Can* fame, who as a teenager began passing bad checks across the nation and eventually around the world before being arrested in France in 1969 and landing in a U.S. federal prison in 1971.

**Financial crime became a pressing priority in the mid-1970s, when Director Clarence Kelley made white-collar crime—which in the fallout of Watergate included public corruption—a top focus of the FBI.** By 1976, Director Kelley noted that 15 percent of our agents were working white-collar crime cases, and the next decade saw the beginning of a wave of agent-intensive, high-dollar, and high-impact financial fraud investigations with our partners that continues to this day. A few examples:

- The savings and loan crisis that arose in the early 1980s became our first massive national financial



In the 1970s, financial fraud cases began to rise, as shown in this excerpt from the 1975 annual report.

fraud probe. By the end of the decade, hundreds of FBI agents were investigating more than 530 banks to determine if fraud or embezzlement were involved in their failures.

- Health care fraud exploded in the early 1990s, leading to more than 100 arrests in our first major case—Operation Gold Pill—in 1992.
- Telemarketing fraud also took off in the 1990s, resulting in significant cases like Operation Disconnect and Operation Senior Sentinel.
- Insider trading scandals made national news in the 1980s with the probes of Ivan Boesky and Michael Milken. The FBI joined its first major investigation of a Wall Street executive soon after, helping to convict powerful municipal finance banker Mark Ferber in 1996.
- The collapse of Enron in 2001 and the ensuing investigation led to a series of major corporate fraud investigations in the following decade.

**The threat remains...and our work goes on.** As evidenced in our latest *Financial Crimes Report*—buttressed by last week’s conviction of Robert Allen Stanford, who misappropriated \$7 billion from his own company—we continue to address the threat of financial fraud...everything from insider trading to insurance fraud, from mortgage fraud to bank failures, from mass marketing scams to health care and corporate fraud.



## Community Leaders Recognized

### Their Actions Improve Lives

An Albuquerque man who devotes his time to educating his community about cyber threats. A Jacksonville woman whose child protection group assists law enforcement with crimes against children cases. An Arizona organization dedicated to meeting the needs of murder victims' families. A man who established a volunteer organization in Delaware to serve at-risk youth.

Since 1990—through the Director's Community Leadership Awards (DCLA)—the FBI has publicly recognized the achievements of individuals and organizations like these who have gone above and beyond the call to service by making extraordinary contributions to their communities in the areas of terrorism, cyber, drug, gang, or violence prevention and education. And this year is no exception: today, nearly 60 individuals and organizational representatives—all 2011 DCLA recipients—gathered for a ceremony in their honor at FBI Headquarters in Washington, D.C.

Director Mueller, who presented a specially designed plaque to each recipient, called the honorees “catalysts for change” in their communities and said that each one shared “a willingness to lead...a commitment to improving your neighborhoods...and a desire to make this country safer for your fellow citizens.”

Each of our field offices is given the chance to present the award at the local level during the year, and the honorees are then recognized at the annual national ceremony the following spring. FBI Headquarters selects at least one winner as well. A snapshot of this year's DCLA recipients shows the range of good work done across the nation:

- **Anchorage:** Covenant House Alaska offers services to homeless, runaway, and at-risk youth and has been an essential partner of the FBI on our Innocence Lost Task Force and human trafficking cases.
- **Boston:** Ted Woo is a member of BRIDGES (Building Respect in Diverse Groups to Enhance Sensitivity), a group of law enforcement and community leaders who work together on community concerns. Among other activities, Woo has coordinated several community events held in mosques and gurdwaras.
- **Chicago:** Brent King, whose daughter was kidnapped and murdered by a convicted sex offender, established a non-profit foundation dedicated to working with state legislatures to toughen restrictions on violent sexual predators.
- **Jackson:** Federal Judge James Graves, Jr. is deeply committed to teaching, motivating, and inspiring Mississippi youth. He also mentors young people about the legal system.
- **Kansas City:** Marvin Szneler is the executive director of a Jewish organization that works to build relationships among various religious and community groups, government officials, law enforcement, educators, and the media.
- **Miami:** Essie Reed is the founder of Team of Life, Inc., an organization that serves at-risk children by providing meals, clothing, and transportation and encourages young people to help law enforcement reduce crime, drug abuse, and violence in their communities.
- **Portland:** Musse Olol, head of the Somali American Council of Oregon, assists Somali refugees by serving as an interpreter, facilitator, counselor, and co-sponsor and helps establish positive relationships between the Somali community and state and federal law enforcement.
- **Tampa:** Rose Ferlita established Bully Busters, a national anti-bullying program involving partnerships among young people, parents, local law enforcement, and community groups.

Congratulations to all the winners. It's our hope that their selfless actions to enhance the lives of neighbors and protect communities will inspire others to offer their time and talents to their own communities.



# Eco-Terrorist Sentenced

## Help Us Find Remaining Operation Backfire Fugitives

After he was indicted in 2006 for firebombing a University of Washington research facility, Justin Solondz became an international fugitive, beginning an odyssey that would land him in a Chinese jail—and finally before a federal judge in Seattle, who sentenced him last week to seven years in prison.

Solondz, 32, was a member of an eco-terrorist cell known as “The Family,” which committed an estimated \$48 million worth of arson and vandalism across the Pacific Northwest and western U.S. between 1996 and 2001 under the names of the Animal Liberation Front and the Earth Liberation Front.

**Three members of The Family are still on the run, and there is a reward for information leading to their arrest.**

The cell’s most notorious crime was the 1998 arson of a Vail, Colorado ski resort that caused \$26 million in damages and drew international attention to eco-terrorists—those who break the law in misguided and malicious attempts to protect the environment and animal rights. We took the lead in the Vail investigation, working closely with our local, state, and federal law enforcement counterparts. In 2004, multiple eco-terror investigations were condensed into Operation Backfire.

We need your help to bring the three remaining fugitives from The Family to justice. A reward of up to \$50,000 each is being offered for information leading to the arrest of Joseph Dibee, Josephine Overaker, and Rebecca Rubin, all believed to be living abroad.

### Here is what we know about the trio:

- Dibee was indicted in 2006 on charges of arson, conspiracy, and animal enterprise terrorism. He is believed to be living in Syria with family members.
- Overaker was indicted in 2004 and 2006 for her involvement with the 1998 Vail arson and other crimes. She is believed to have spent time in Germany and may have settled in Spain. She speaks fluent Spanish.
- Rubin was indicted in 2006 for the Vail arson and other acts of domestic terrorism. A Canadian citizen, she has strong family ties to Canada and may be living there.



The 1998 arson of a Colorado ski resort drew international attention to eco-terrorists—those who break the law in misguided and malicious attempts to protect the environment and animal rights.

Investigators identified Solondz as a member of The Family in the spring of 2006, said Special Agent Ted Halla in our Seattle office. “He was traveling overseas, and we started tracking him through Europe to Russia, Mongolia, and then China. He realized we were after him,” Halla said. “He liquidated his bank accounts and tried to hide his tracks online. By the summer of 2006, he disappeared in China.”

Working through our legal attaché office in Beijing, we learned that Solondz had been arrested in China for manufacturing drugs and sentenced to prison. He served nearly three years before the Chinese released him to our custody.

As part of his plea, Solondz admitted building the firebomb that was planted in the office of a University of Washington horticultural researcher. He and The Family mistakenly believed the researcher was genetically altering trees. The fire ruined the researcher’s work along with the work of dozens of other students and researchers.

“The Solondz case has been a long process,” Halla said. “When you are after someone for that many years, it’s a big relief to see the individual finally brought to justice.”



## FBI Financial Intelligence Center

### Getting Ahead of Crime

Investigating financial crime is like working a puzzle—you have to fit all of the pieces of information together in order to see the entire picture. The FBI's Financial Intelligence Center in Washington, D.C. does just that, linking disparate pieces of data to give our field investigators a clearer picture of possible criminal activity in their regions.

The center was established in the fall of 2009 in response to the financial crisis at that time—its mission was to identify potential investigative targets engaged in mortgage fraud. Because of its success, the center's focus expanded to include other types of financial crimes, like securities/commodities fraud, health care fraud, money laundering, fraud against the government, and even public corruption (which usually involves financial wrongdoing of some sort).

**The center is staffed primarily by intelligence analysts and staff operations specialists.** Their first order of business is to review large datasets that come from the FBI, other law enforcement and regulatory agencies, consumer complaint websites, etc. Computer programs cull out data with common themes (i.e., similar scams, similar names). That data is researched and analyzed to help further identify potential subjects and/or activity, and the results are organized using spreadsheets and link analysis to draw connections among all the key players. If there is good reason to believe that criminal activity exists, the results are summarized in an intelligence package and sent to the appropriate field office.

During fiscal year 2011, FBI offices opened dozens of investigations based on the center's intelligence packages.

**Current initiatives.** In response to some of the most serious financial crimes, the Financial Intelligence Center is working on a number of specific initiatives, such as:

- Foreclosure rescue fraud, where analysts collect and evaluate deceptive practices complaint data from the Federal Trade Commission (FTC), which is then cross-referenced with suspicious activity reports filed by financial institutions;
- Securities and corporate fraud, in which the center partners with the Commodities and Futures Trading Commission and Securities and Exchange Commission (SEC) to review civil referrals for possible criminal violations;
- Health care fraud, which involves us working with the Centers for Medicare and Medicaid (CMS) and the Department of Justice on a new predictive modeling system that uses algorithms to generate lists of medical professionals potentially engaging in health care fraud; and
- Money laundering, in which analysts review incoming intelligence from the FBI's Southwest Border Initiative to determine if subjects are laundering proceeds from criminal activities.

Although the center's primary mission is to identify those who may have thus far escaped the law enforcement lens, it also uses its tools and expertise to enhance current investigations that feature large numbers of subjects and multiple FBI offices.

**Of course, we don't do this alone—we work closely with our partners.** As a matter of fact, our analysts are currently or will soon be embedded in the Office of the Special Inspector General for the Troubled Asset Relief Program, the SEC, the Internal Revenue Service, the FTC, and the CMS....to expand even further the pool of data that can be used by all to uncover financial crime.

The bottom line of the FBI's Financial Intelligence Center: to work proactively to help identify the nation's most egregious criminal enterprises.

# The Cyber Threat

## Part 1: On the Front Lines with Shawn Henry

*Note: Shawn Henry retired from the FBI on March 31, 2012.*

Shawn Henry realized a lifelong dream when he became a special agent in 1989. Since then, he has traveled the world for investigations and become one of the FBI's most senior executives and its top official on cyber crime. FBI.gov recently sat down with Henry—who is about to retire from the Bureau—to talk about the cyber threat and his FBI career.

**Q:** You were involved with cyber investigations long before the public had an awareness of how serious the threat is. How did you become interested in the cyber realm?

**Mr. Henry:** I was always interested in technology, and in the late 1990s I started to take courses at the FBI related to cyber intrusion investigations. When I had an opportunity to move over to that side of the house, I seized it. I saw right away that the challenges we were going to face in the future were tremendous, and I wanted to be on the front lines of that.

**Q:** How has the cyber threat changed over time?

**Mr. Henry:** Early on, cyber intrusions such as website defacements and denial of service attacks were generally perceived to be pranks by teenagers. But even then, in the late 1990s, there were state actors sponsored by governments who were attacking networks. What received media attention was the teenage hacker and the defacements, but there were more significant types of attacks and a more substantial threat that was in the background. Also, those early attacks were much more intermittent. Now we are seeing literally thousands of attacks a day. The ones people hear about are often because victims are coming forward. And there are more substantial attacks that people don't ever see or hear about.

**Q:** Where are the cyber threats coming from today?

**Mr. Henry:** We see three primary actors: organized crime groups that are primarily threatening the financial services sector, and they are expanding the scope of their attacks; state sponsors—foreign governments that are interested in pilfering data, including intellectual property and research and development data from major manufacturers, government agencies, and defense contractors; and increasingly terrorist groups who want to impact this



Shawn Henry, executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch.

country the same way they did on 9/11 by flying planes into buildings. They are seeking to use the network to challenge the United States by looking at critical infrastructure to disrupt or harm the viability of our way of life.

**Q:** How has the FBI adapted to address the threat?

**Mr. Henry:** We have grown substantially, particularly in the last four or five years, where we have hired more technically proficient agents, many of whom have advanced degrees in computer science or information technology. We bring them onboard and teach them to be FBI agents rather than trying to teach FBI agents how the technology works. That has given us a leg up and put our capabilities on par with anybody in the world. We have also worked proactively to mitigate the threat by using some of the same investigative techniques we use in the physical world—undercover operations, cooperating witnesses, and authorized surveillance techniques. We have taken those same time-tested tactics and applied them to the cyber threat. So we are now able to breach networks of criminal actors by putting somebody into their group. The other critical area we have been successful in is developing partnerships.

*Part 2: Why partnerships are so important (page 26)*





## The Cyber Threat

### Part 2: Shawn Henry on Partnerships, Challenges

*Note: Shawn Henry retired from the FBI on March 31, 2012.*

*Part 2 of an interview with Shawn Henry, executive assistant director of the Criminal, Cyber, Response, and Services Branch.*

#### **Q: Why are partnerships so important?**

**Mr. Henry:** The threat we face is not solely within the FBI's area of responsibility. So we work very closely with other law enforcement agencies and the intelligence community domestically. We share tactics and intelligence. We also partner with the private sector, because they often are the victims and see attacks before anybody else. The final piece—and one of the most significant—is international law enforcement partnerships. The ability to reach across the ocean once we identify criminals and put our hands on them is something that is relatively new. For many years, the adversaries believed they were immune to prosecution because they were thousands of miles away. That's not the case anymore. Through our partnerships, we have arrested hundreds of bad actors who targeted U.S. and foreign infrastructure and institutions. Just in the last two years we have worked with dozens of countries, and we have actually stationed FBI agents overseas into the police agencies in countries including Ukraine, Romania, The Netherlands, and Estonia.

#### **Q: So the cyber threat is truly global in scope?**

**Mr. Henry:** Absolutely. In the physical world when somebody robs a bank, the pool of suspects is limited to the number of people in the general vicinity of that bank. When a bank is robbed virtually, even though it is very

real for the victims—the money is actually gone—the pool of suspects is limited to the number of people on the face of the earth that have a laptop and an Internet connection, because anybody with an Internet connection can potentially attack any other computer that is tied to the network. You don't have to be a computer scientist to launch these types of attacks.

#### **Q: Going forward, what are the challenges regarding the cyber threat?**

**Mr. Henry:** What I call the expansion of the network is going to create challenges. As technology increases, the threat becomes greater. All our wireless networks and smart devices are network-based, and anything touching the network is potentially susceptible. As more and more information transitions across the network, more adversaries will move to get their hands on it, because that information is extraordinarily valuable.

#### **Q: You have responsibilities beyond the cyber area. What are some of the challenges you see with other criminal matters?**

**Mr. Henry:** As an organization, fighting terrorism is rightfully the FBI's number one priority, but criminal threats are substantial. There is white-collar crime, where we've seen people lose their entire life savings because of criminals taking advantage of them. There's something very rewarding about seeing our agents and analysts aggressively working to take those criminals off the streets. We've seen public corruption cases where people have abused their position for personal gain. I see those types of cases continuing. There's a percentage of people in society that are always going to be bad actors.

#### **Q: What are you going to miss when you leave the Bureau?**

**Mr. Henry:** The people and the mission. There is nothing else I wanted to do more in my professional life than to be an FBI agent. The quality and caliber of the people I have worked with are second to none. Working day to day to carry out our mission to help protect the country is an experience that can never be replaced. I leave with a tremendous sense of pride.

# The Grandparent Scam

## Don't Let It Happen to You

You're a grandparent, and you get a phone call or an e-mail from someone who identifies himself as your grandson. "I've been arrested in another country," he says, "and need money wired quickly to pay my bail. And oh by the way, don't tell my mom or dad because they'll only get upset!"

This is an example of what's come to be known as "the grandparent scam"—yet another fraud that preys on the elderly, this time by taking advantage of their love and concern for their grandchildren.

**The grandparent scam has been around for a few years**—our Internet Crime Complaint Center (IC3) has been receiving reports about it since 2008. But the scam and scam artists have become more sophisticated. Thanks to the Internet and social networking sites, a criminal can sometimes uncover personal information about their targets, which makes the impersonations more believable. For example, the actual grandson may mention on his social networking site that he's a photographer who often travels to Mexico. When contacting the grandparents, the phony grandson will say he's calling from Mexico, where someone stole his camera equipment and passport.

### Common scenarios include:

- A grandparent receives a phone call (or sometimes an e-mail) from a "grandchild." If it is a phone call, it's often late at night or early in the morning when most people aren't thinking that clearly. Usually, the person claims to be traveling in a foreign country and has gotten into a bad situation, like being arrested for drugs, getting in a car accident, or being mugged... and needs money wired ASAP. And the caller doesn't want his or her parents told.
- Sometimes, instead of the "grandchild" making the phone call, the criminal pretends to be an arresting police officer, a lawyer, a doctor at a hospital, or some other person. And we've also received complaints about the phony grandchild talking first and then handing the phone over to an accomplice...to further spin the fake tale.
- We've also seen military families victimized: after perusing a soldier's social networking site, a con artist will contact the soldier's grandparents, sometimes claiming that a problem came up during military leave that requires money to address.



- While it's commonly called the grandparent scam, criminals may also claim to be a family friend, a niece or nephew, or another family member.

**What to do if you have been scammed.** The financial losses in these cases—while they can be substantial for an individual, usually several thousand dollars per victim—typically don't meet the FBI's financial thresholds for opening an investigation. We recommend contacting your local authorities or state consumer protection agency if you think you've been victimized. We also suggest you file a complaint with IC3 ([www.ic3.gov](http://www.ic3.gov)), which not only forwards complaints to the appropriate agencies, but also collates and analyzes the data—looking for common threads that link complaints and help identify the culprits.

### And, our advice to avoid being victimized in the first place:

- Resist the pressure to act quickly.
- Try to contact your grandchild or another family member to determine whether or not the call is legitimate.
- Never wire money based on a request made over the phone or in an e-mail...especially overseas. Wiring money is like giving cash—once you send it, you can't get it back.



Left: FBI Director Robert S. Mueller addresses the Miami Chamber of Commerce.

## Major Financial Crime

### Using Intelligence and Partnerships to Fight Fraud Smarter

Homeowners tricked into signing away the deeds to their own homes. The elderly and vulnerable used to make a fast and illegal buck, even by the very people who take care of them. Billions in hard-earned investor dollars vanishing in a seeming flash, sometimes through a single scam.

**Financial crime is a real and insidious threat—one that takes a significant toll on the economy and its many victims.** Today, Director Robert S. Mueller talked about the impact of financial crime and the Bureau's longstanding role in combating it in a keynote speech before the Miami Chamber of Commerce.

The Director explained that even in the post-9/11 world—with its needed focus on terrorism and other national security threats—the FBI continues to take its criminal responsibilities seriously. "What has changed," he said, "is that we make greater use of intelligence and partnerships to better focus our limited resources where we can have the greatest impact—for example, on combating large-scale financial fraud."

It's all about working smarter—using new information-sharing efforts, intelligence-driven investigations, and task force-based approaches to leverage the talents and resources within and among agencies to get a bigger bang for the buck, so to speak, in fighting financial fraud.

**Among the innovations and initiatives outlined by the Director:**

- Three years ago, we established the Financial Intelligence Center to strengthen our financial intelligence collection and analysis. "This center helps us to see the entire picture of financial crimes. It provides tactical analysis of financial intelligence data, identifies potential criminal enterprises, and enhances investigations. It also coordinates with FBI field offices to complement their resources and to identify emerging economic threats."
- Today, we have more than 500 agents and analysts using intelligence to identify emerging health care fraud schemes, and field offices target fraud through coordinated initiatives, task forces and strike teams, and undercover operations.
- The Miami office has led the way by creating the first Health Care Fraud Strike Force, which is now a national initiative. Through the strike force, the Bureau works closely with federal, state, local, and private sector partners to uncover fraud and recover taxpayer funds. "Last year, our combined efforts returned \$4.1 billion dollars to the U.S. Treasury, to Medicare, and to other victims of fraud."
- As the result of a new forensic accountant program, we now have 250 forensic accountants "trained to catch financial criminals" and "ready to respond quickly to high-profile financial investigations across the country."
- In the last four years, we have nearly tripled the number of special agents investigating mortgage fraud. "Our agents and analysts are using intelligence, surveillance, computer analysis, and undercover operations to identify emerging trends and to find the key players behind large-scale mortgage fraud."
- In 2010, the FBI began embedding agents at the Securities and Exchange Commission (SEC). "This allows us to see tips about securities fraud as they come into the SEC's complaint center...to identify fraud trends more quickly and to push intelligence to our field offices."

**Everyone has a role in fighting fraud, including business and community leaders.** "You can learn to recognize financial fraud and unscrupulous business practices, to better protect yourself and your companies," Mueller said. "And you can alert us when you see these activities take place."



# New Top Ten Fugitive Child Pornographer Added to the List

Eric Justin Toth, a former private-school teacher and camp counselor accused of possessing and producing child pornography, is the newest addition to the FBI's Ten Most Wanted Fugitives list.

**Toth, who also goes by the name David Bussone, has been on the run since warrants for his arrest were issued in Maryland and the District of Columbia in 2008.** There is a reward of up to \$100,000 for information leading directly to Toth's arrest, and we need your help to locate him.

"We have always counted on the public's support to help capture fugitives and solve cases," said Michael Kortan, assistant director of our Office of Public Affairs. "The addition of Eric Toth to the Top Ten list illustrates how important it is to get this individual off the streets and into custody."

Our investigation began in June 2008, after pornographic images were found on a camera that had been in Toth's possession at the private school where he worked. Since becoming a fugitive, he is believed to have traveled to Illinois, Indiana, Wisconsin, and Minnesota. Investigators believe he lived in Arizona as recently as 2009.

**Toth turned 30 on February 13. He is 6'3" tall and weighs about 155 pounds.** He has brown hair, green eyes, and a medium complexion. He has a mole under his left eye.

Toth is well educated—he attended Cornell University for a year and then transferred to Purdue University, where he earned an education degree. He is described as a computer expert and is believed to regularly use the Internet and social networking websites. He may advertise online as a tutor or male nanny.

Since its creation in 1950, the Top Ten list has been invaluable to the FBI, helping us capture some of the nation's most dangerous criminals. Of the 495 fugitives named to the list, 465 have been apprehended or located. That level of success would not be possible without the strong support of the public, whose help has led to the capture of 153 of the Top Ten fugitives.

Over the years, we have created several digital tools to spread the word about our fugitives program, including a widget that can be added to anyone's website or blog. The



**Eric Justin Toth, a former private-school teacher and camp counselor, has been on the run since warrants for his arrest were issued in Maryland and the District of Columbia in 2008.**

widget is an interactive application featuring information on all Top Ten fugitives, along with continuous feeds of FBI news and stories that are automatically updated. It's easy to add to almost any website, including Facebook and other social networking sites, and it currently appears on hundreds of websites around the world.

In addition, more than 60,000 people subscribe to our Ten Most Wanted Fugitives category through e-mail updates and listen to our Wanted by the FBI podcasts. The Wanted by the FBI section on our website is viewed by over a million people every month. Also, our National Digital Billboard Initiative partners, who currently have 3,200 billboards in 42 states, are donating space to help publicize the newest Top Ten fugitive.

**Our modern electronic methods allow us to reach more people than ever, but we still need your help.**

If you have any information about Eric Justin Toth—or any of the fugitives on our Top Ten list—please contact your local FBI office or submit a tip electronically on our website at <https://tips.fbi.gov>.



Scan this QR code with your smartphone to watch a related video, or visit <http://www.fbi.gov/news/videos/>.



## Bankruptcy Fraud

### Creditors and Consumers Pay the Price

Federal bankruptcy proceedings can be a lifesaver for honest individuals overwhelmed by debt as a result of unemployment, a medical crisis, divorce, disability, or any number of other legitimate reasons.

Unfortunately, bankruptcy can also be used by the unscrupulous to get out of paying their debts...even though they may have the financial assets to do so. And often, financial fraudsters use bankruptcy filings to prolong their illegal white-collar schemes—buying time before the game is up for good.

**The FBI is the primary investigative agency responsible for addressing bankruptcy fraud.** And while there are other financial crimes that require larger investments of our resources—like mortgage, financial institution, and health care fraud—we take our responsibility to pursue allegations of bankruptcy fraud very seriously. We focus on cases with large dollar amounts, the possible involvement of organized crime, and suspects who file in multiple states. Currently, we have nearly 300 pending bankruptcy fraud cases open around the country.

**How the process begins.** The U.S. Trustees Program, part of the Department of Justice, oversees the bankruptcy system. When it uncovers suspected fraud, it refers the information to the appropriate U.S. attorney and to the FBI. Working closely with the U.S. Attorney's Office, our investigators open a case if warranted and begin conducting interviews and reviewing financial documents. Based on the complexity of the case, we can also use techniques like undercover operations and court-authorized electronic surveillance to gather more evidence.

**The culprits.** They typically include private citizens, small business owners, corporate CEOs, real estate agents, politicians, and loan officers. We've even seen cases where bankruptcy attorneys and bankruptcy petition preparers have engaged in criminal behavior at the expense of debtors and creditors in bankruptcy proceedings.

**The most common types of bankruptcy fraud.** The majority of our casework involves people who have lied under oath or provided false documentation during their bankruptcy proceedings, concealed or transferred their financial assets, or committed tax fraud. Other schemes include using false identities to file for bankruptcy multiple times in multiple locations, bribing a bankruptcy trustee, and intentionally running up credit card bills with no intention of paying them off (also known as "credit card bust-outs").

Our investigations have shown that many times bankruptcy fraud is committed in conjunction with crimes such as credit card fraud, identity theft, mortgage fraud, money laundering, mail and wire fraud, etc.

**The FBI often partners with other federal agencies—like the Internal Revenue Service—to investigate bankruptcy fraud.** We also participate in many of the 70-plus bankruptcy fraud/mortgage fraud working groups and specialized task forces around the country...with U.S. Trustee Program representatives, U.S. attorneys, and other federal partners.

Bankruptcy fraud not only affects creditors like businesses and financial institutions who lose money from fraud, it also results in higher credit card and loan fees and often higher taxes...for everyone. So if you suspect bankruptcy fraud, please contact the U.S. Trustees Program at USTP. Bankruptcy.Fraud@usdoj.gov or your local FBI office.

If you are considering filing for bankruptcy for legitimate reasons, contact an attorney who specializes in bankruptcies—and do your due diligence before hiring a lawyer by getting referrals from someone you know who has declared bankruptcy, checking with your local bankruptcy court, contacting your state bar association, etc.

## ‘Booster’ Behind Bars

### Professional Shoplifter Gets Prison Term

An Oregon man described by prosecutors as a professional shoplifter was recently sentenced to a year and a day in federal prison in a case that illustrates the serious problem of retail theft at the hands of so-called “boosters.”

**John Patrick Weismiller was sentenced in March for shoplifting from Portland-area retail stores and then selling the stolen merchandise on eBay for a handsome profit.** In the seven-month period between January and July 2011, he repeatedly visited Oregon stores such as Safeway, Target, and Best Buy and boosted health and beauty products, over-the-counter pharmaceuticals, and other items—usually by stuffing the products under his clothing.

Weismiller then sold the stolen merchandise online, often at half the price of its retail value. During that seven-month period, he earned \$43,200, which represented more than \$73,000 in retail losses.

Our organized retail theft program at FBI Headquarters focuses on the most significant retail theft cases involving the interstate transportation of stolen property. In most instances, these investigations involve organized theft groups, but Weismiller’s case was different because he was a lone operator.

“Normally, a single booster like this is handled by local law enforcement,” said Special Agent Joe Boyer, who works out of our Portland Field Office. “But when we have this kind of prolific thief and the U.S. Attorney is willing to prosecute the case, the FBI is happy to get involved.”

Boyer noted that most professional boosters have little fear of going to jail for retail theft, because their crimes are non-violent. Often when a booster is caught shoplifting from a retail store, he or she is cited with a fine and released.

**Safeway’s loss prevention team documented Weismiller stealing merchandise from its stores 105 times in early 2011.** Despite being stopped and forbidden to return to Safeway outlets in July 2011, he was observed just two days later shoplifting at a different Safeway store. Prosecutors noted that between May 2006 and May 2011, the 41-year-old Weismiller listed 6,681 items for sale on eBay, including hundreds of packages of Crest Whitestrips.



**During a seven-month stretch of shoplifting, John Patrick Weismiller earned \$43,200, which represented more than \$73,000 in retail losses. He re-sold merchandise through online auctions.**

Working with Safeway’s loss prevention personnel and local law enforcement, FBI agents were able to tie the stolen goods and online sales to Weismiller. He pled guilty to the thefts and, after his prison sentence, must serve three years of supervised release and pay restitution of nearly \$21,000.

**“Law-abiding citizens bear the cost of organized retail theft every time they make a purchase, paying a higher cost for goods than they would otherwise,”** said Greg Fowler, special agent in charge of our Portland office. “The FBI and its retail partners work to disrupt these groups by identifying and investigating the most egregious offenders and insuring they are held accountable.”

“This guy was incredibly brazen,” Special Agent Boyer said. “He was making his living doing this. This was his full-time job. He lived in a nice house in the suburbs with his wife and kids. If you lived next door,” he said, “you would have no idea he was a thief.”

Boyer added, “The fact that Weismiller is now in prison should send a message to other boosters who think they are flying under the legal radar: the FBI is serious about these crimes, and professional shoplifters will end up behind bars.”





**Left: A child forensic interviewer watches on closed-circuit television as a police officer talks to a victim during a mock interview. In addition to supporting investigations, the interviewers provide specialized training to FBI agents and law enforcement partners around the world.**

## Child Forensic Interviewers

### Part 1: Providing Critical Skills on Sensitive Investigations

An 11-year-old who witnessed a murder. A terrified teenager who watched her parent beat and lock her sister in a closet over a period of weeks. A 12-year-old lured by two men on the Internet to a rendezvous where she was raped.

**In all these tragic cases, children were either witnesses to or victims of crimes. The ability to get them to talk about what they saw and experienced is the job of our child forensic interviewers, whose expertise is in constant demand across the country.**

“Traditional law enforcement interviewing methods used in typical adult cases are counterproductive when it comes to child victims or witnesses to crimes,” said Stephanie Knapp, one of the Bureau’s four child forensic interviewers. “Sometimes you see unsuccessful outcomes in cases because of poor interview techniques. In many cases of child abuse, for example, where the victim is the only witness, the interview may be a critical element of the investigation.”

Part of our Office for Victim Assistance, based at FBI Headquarters, child forensic interviewers specialize in crimes involving human trafficking, child sexual exploitation, and violent crimes, including those on Indian reservations. Like her colleagues—two more members will soon be added to the team—Knapp is a licensed clinical social worker and a highly trained interviewer. While her goal is to support criminal investigations, “we must also consider the unique developmental and emotional needs

of victims and witnesses,” she said. “There is a delicate balance between doing what’s best for victims and what’s best for cases.”

The actual interview techniques are built on a set of research-based protocols. “Our techniques are very effective,” said interviewer Karen Blackwell. “We often get case-breaking information after traditional methods have failed.”

The team conducts hundreds of interviews nationwide every year, and it also trains others—an important part of the mission. “We can’t possibly handle all the interview requests we get,” Knapp said. “So we train law enforcement officers domestically and internationally on our techniques.”

**Although they follow time-tested protocols, interviewers acknowledge that working with children is an art as well as a science, requiring experience and intuition.** “You have to understand and follow the protocols,” Blackwell said, “but it’s also essential that you connect with the kids so that they trust you.”

Often, interviewers don’t have much time to establish that trust, and it may have to happen through an interpreter. Sometimes—because they are afraid or have learned not to trust adults—“the kids just aren’t ready to talk,” Blackwell said. “You have to deal with that.”

“We often see the worst of humanity,” Knapp explained. “But we also have the opportunity to have a positive impact on the life of a traumatized child by simply listening to them talk about their trauma. This can be amazingly powerful and helpful to the healing process.”

“We know kids don’t always tell us everything during interviews,” she added. “But disclosure is a process, and part of our job is to help investigators understand why a victim may or may not be disclosing information. On some level, many of these children are struggling to survive.”

Success isn’t always defined by a positive prosecution, Knapp noted. “Success must also include helping children understand that they do not have to define themselves as victims for the rest of their lives because of the trauma or abuse they may have suffered.”

*Part 2: Training is essential to the mission (page 33)*

# Child Forensic Interviewers

## Part 2: Training Our Law Enforcement Partners

In a makeshift interview room in Northern Virginia, a girl was asked to describe how she became a crime victim. An older man she met on the Internet lured her into sending him nude pictures. And now an investigator was trying to build a case against the man.

In this scenario, the girl was an actress playing an underage teen and the investigator was an international police officer attending a two-week human trafficking course at the FBI Academy in Quantico. A key piece of the curriculum was learning how to properly interview child victims using techniques practiced by the child forensic interviewers in the FBI's Office for Victim Assistance (OVA), where a forensic interviewer's primary role is to further an investigation.

**"The forensic interview is to gather statements that can be used in court," said Martha Finnegan, one of four FBI child forensic interviewers who have developed a proven approach to questioning kids following crimes and traumatic events. "We actually have a research-based protocol that we follow that consists of multiple stages. And following the protocol makes the interview legally defensible in a court of law."**

Knowing what to ask—and what not to ask—is essential, as is knowing how to get young crime victims to open up. The recent training was for 17 law enforcement officers from four Central American countries. They were led through scenarios covering everything from where to conduct interviews and who should attend to how to open conversations and put young victims at ease.

The officers learned different techniques for building rapport with young children and older adolescents, all the while being reminded to balance investigative efforts against the conditions of the victims.

**"One of the most important things, besides getting the information and the evidence, is also to do it in a way that doesn't additionally traumatize that child," said Kathryn Turman, program director for OVA. "We've actually found that it can be empowering to a child to be able to tell what happened and to be able to tell it soon."**

Mock interviews follow the two days of lectures. The officers, assisted by Spanish-speaking FBI interpreters,



**An actress portraying a young crime victim is interviewed during an FBI workshop on human trafficking. The exercise was designed to instruct law enforcement officers visiting from Central America on how we conduct forensic interviews with children and adolescents.**

paired off with actors trained to exhibit specific victim behaviors, which included being less than cooperative. These officers spend their days facing down gang members and dangerous criminals, but quite often children are around when crimes occur. "So being able to talk to kids who are present in so many different situations is really a great skill to have," Turman said.

In a room adjoining the interviews, classmates watched on closed-circuit television as their colleagues took turns trying to apply the protocol they just learned to a realistic interview. The underage girl who was solicited to send nude pictures was stoic and evasive, compelling her interviewer to modify his line of questioning until finally he made a connection. Each officer got to conduct two separate interviews, and each showed a marked improvement.

**The FBI child forensic interviewers conduct scores of interviews each year and provide training and technical assistance to thousands of local, state, and federal partners.** Finnegan said she hopes the officers will apply and share the FBI's approach back home and keep evolving their skills.

"We're hoping that they're able to take some parts of our protocol and some understanding about the dynamics of exploitation away from this training," she said.



Scan this QR code with your smartphone to watch a related video, or visit <http://www.fbi.gov/news/videos/>.



Left: Dolce, the FBI's first and only therapy dog.

## Helping Victims of Crime Therapy Dog Program a First for the Bureau

Rachel Pierce is a victim specialist in our Office for Victim Assistance. Her partner is an 8-year-old German Shepherd/Siberian Husky mix, and together they form a unique and remarkable team.

**The FBI uses a variety of working dogs—highly capable canines that can sniff out drugs and bombs, bolster security, and alert their handlers when they pick up the scent of blood. But Dolce, with his shimmering yellow coat and steel blue eyes, is the Bureau's one and only therapy dog.**

The job of a victim specialist, or VS, is to ensure that victims receive the rights they are entitled to under federal law and the assistance they need to cope with crime. With his lovable personality, Dolce excels at comforting crime victims and their families. The story of how he became a VS—of the K-9 variety—is a story in itself.

Pierce, a psychologist who worked for the Department of Defense and law enforcement before joining the Bureau about five years ago, suffers from rheumatoid arthritis, a chronic inflammatory disease whose symptoms can be debilitating when they strike. In 2004, she went to a local shelter looking for a puppy she could train to be a service dog. That's where she found Dolce.

"I thought it would be nice to have a dog that did some things around the house for me when my symptoms flared up," she said. "There are days I can't move or even lift a sheet."

After extensive service dog training, Dolce learned how to turn light switches on and off, load laundry in the

washing machine, and even retrieve drinks from the refrigerator. "He is a very good service dog," said Pierce, who is based in our Nashville Resident Agency. "But service dogs are not supposed to interact with the public."

**That was a problem, because Dolce loves people. Pierce soon realized that Dolce's intelligence and temperament would make him a terrific therapy dog.** She knew from her military experience that the Army has a successful therapy dog program, and she set out to introduce a something similar at the FBI.

On her own, Pierce undertook an extensive training regimen with Dolce, and he passed registration exams given by Pet Partners and other organizations. In 2009, after spending many volunteer hours taking Dolce to nursing homes, camps for grieving children, and other places that use therapy dogs, Pierce's proposal for the K-9 Assisted Victim Assistance Program was approved by the FBI and adopted as a pilot program.

Since then, she and Dolce have had a very positive impact, comforting victims and their families in murder cases, kidnappings, and bank robberies, where Dolce's presence is a calming influence on tellers who minutes before may have had a gun pointed in their faces.

Studies have shown that the presence of an animal in a stressful situation can produce a calming effect, Pierce said. "It can lower blood pressure and make you feel more relaxed." In the immediate aftermath of a bank robbery, for example, a calm witness can better relay information about the crime to investigators.

"We have worked a lot of cases together," Pierce said, "helping victims of child pornography and even white-collar crime, where senior citizens lost their life savings to investment scam artists. Dolce has helped a lot of people," she added. "I am so proud of him for all the lives he has touched in a positive way."



Scan this QR code with your smartphone  
to watch a video about Dolce, or visit  
<http://www.fbi.gov/news/videos/>.



## A Byte Out of History

### The Alvin Karpis Capture

Mr. O'Hara certainly liked to fish. He had gone out almost every day, according to the superintendent of his apartment building in New Orleans. O'Hara had shown up in the Big Easy with some friends about a month earlier—in April 1936—but often traveled out of town to visit prime fishing haunts until his cash dwindled.

**O'Hara was no ordinary angler.** His real name was Alvin "Creepy" Karpis, and he was a big fish himself—the most wanted man in America, one of the smartest of the Depression-era gangsters and one of the few still on the run. That was about to end. On May 1, 1936—76 years ago today—Director J. Edgar Hoover and his increasingly capable group of agents were poised to reel him in.

Karpis had long led a life a crime. He was born in Montreal in 1907 under the name Karpavicz; his parents—immigrants from Lithuania—later settled down in Kansas. In 1926, he found himself serving 10 years in prison for burglary. Following a jail-break in 1930, Karpis began his criminal career in earnest, often working with members of the Barker family, all of whom were habitual criminals. A string of bank robberies, auto thefts, and even murder followed.

In 1933, Karpis, his Barker colleagues, and the rest of their gang turned to kidnapping, perhaps seeing the ransom demands as a route to easier and less dangerous money. On June 15, 1933, they snatched Minnesota brewer William Hamm and quickly made \$100,000. Six months later, they abducted St. Paul banker Edward Bremer and demanded \$200,000.

**By early 1935, the ensuing investigation led to the arrest or deaths of most key members of the Barker/Karpis gang.** But not Karpis himself, who managed to elude the FBI and even went to the lengths of having an underworld surgeon alter his fingertips so his prints wouldn't be recognized.

In April 1936, Tennessee Senator Kenneth McKellar called Director Hoover on the carpet during an appropriations hearing, complaining about his request for more funds. When the senator challenged Hoover on how many arrests he had made personally, the Director vowed to himself that he would be involved in the next big one.

**So when word came that Karpis had been located, Hoover flew that night to New Orleans and joined the**



FBI Director J. Edgar Hoover, left, after the arrest of Alvin Karpis.

**waiting raid team, which had staked out the criminals' apartment on Canal Street.** The next day, shortly after 5 p.m., Karpis and two others left the apartment and got in a Plymouth coupe. Hoover signaled his men, who closed in. The Director ordered Karpis to be cuffed. Ironically, no one had brought handcuffs, so one agent removed his tie and secured the hands of Alvin Karpis. The fish had been caught.

Within hours, Hoover was escorting Karpis back to St. Paul, where he eventually pled guilty to the Hamm kidnapping and was sentenced to life in prison. After stays in Alcatraz and other prisons, Karpis was paroled in the late 1960s.

**Hoover's first arrest marked the end of an era, putting behind bars the last of the major gangsters of the 1930s and helping to cement the reputation of the FBI and his own standing.** He would go on to lead the Bureau for exactly 36 more years, dying in his sleep on May 2, 1972.



Left: J. Edgar Hoover's body lies in state in the U.S. Capitol in 1972—an honor afforded to no other civil servant before or since. Hoover died 40 years ago this week. *AP photo*

## The Hoover Legacy, 40 Years After

### Part 1: The End of an Era

He had led the FBI for nearly a half-century and worked for eight different presidents, becoming practically an institution in his own right.

So when J. Edgar Hoover's body was found by his housekeeper on the morning of May 2, 1972—40 years ago this week—the reaction was swift and far-reaching.

Later that day, President Richard Nixon called a press conference to announce the Director's death, saying, "Every American, in my opinion, owes J. Edgar Hoover a great debt for building the FBI into the finest law enforcement organization in the entire world." Nixon ordered that all flags at government buildings be flown at half-staff and spoke at Hoover's funeral two days later.

Congress responded quickly as well, ordering Hoover's body to lie in state in the U.S. Capitol—an honor afforded to no other civil servant before or since. The next day, as rain fell on Washington, thousands processed by his casket in the rotunda to pay their respects, and Supreme Court Justice Warren Burger eulogized the departed Director. Allies and admirers took to the floor of Congress to offer often effusive praise, and a new FBI building on Pennsylvania Avenue, halfway between the Capitol and the White House, was soon named in his honor.

At the same time, as the inevitable obituaries were written and TV specials aired, there was an undercurrent of reservation and some outright criticism. Hoover's historic 48-year tenure in such a position of

profound influence—and during a stretch of time when America was undergoing great social change—was bound to be marked by some mistakes and controversy. Fairly or unfairly, Hoover was criticized for his aggressive use of surveillance, his perceived reluctance to tackle civil rights crimes, his reputation for collecting and using information about U.S. leaders, and his seeming obsession with the threat of communism.

Both feared and beloved within his own organization, Hoover was clearly a complex and often confounding character.

He joined the Department of Justice in 1917 at the tender age of 22 and quickly became a rising star. Hoover was tapped by the attorney general to head the Bureau in 1924, when it was a relatively unknown organization

mired in political scandal. Hard-working, smart, and a superb bureaucrat, Hoover took a fledgling organization and molded it into an international leader in law enforcement and national security, one solidly grounded in professionalism and the techniques of modern science. As the Bureau put the trigger-happy gangsters of the 1930s out of business and outsmarted the spies and saboteurs of World War II, the FBI—and its newly christened "G-Men"—became a household name. Hoover rode that wave of fame, earning widespread acclaim as the nation's top lawman.

The country's honeymoon with Hoover would ultimately come to an end, to some degree in the years before his passing and even more so after his death in the wake of greater scrutiny of the FBI and the growing distrust of government leaders that followed Watergate. Over the next several months, FBI.gov will explore various aspects of the directorship of J. Edgar Hoover through a series of stories and other materials, with the goal of shedding light on lesser-known or even caricatured areas of his actions and broadening the discussion on his complex and enduring legacy.

*Part 2: Hoover's first job and the FBI files (page 54)*



J. Edgar Hoover

# Nursing Home Abuse

## Owner Cheats Government and Neglects Residents

Not enough food. Little air conditioning or heat. Roofs leaking to the point that barrels and plastic sheets were used to catch rain water. Trash piled up in dumpsters. Flies and rodents everywhere, along with rampant mold and mildew.

These were just some of the horrible conditions that elderly residents of three Georgia nursing homes lived under for several years.

The primary culprit? The owner of these homes who, despite having received more than \$32.9 million in payments from Medicare and Medicaid for residents' care, elected to pocket much of the money instead.

**But he didn't get away with it.** Earlier this month, George Dayln Houser was convicted in Atlanta of defrauding Medicare and Medicaid. Houser's accomplice and wife, Rhonda Washington Houser, pled guilty last December.

To receive Medicare and Medicaid payments, Houser agreed to provide his residents with a safe and clean physical environment, nutritional meals, medical care, and other assistance. But as complaints began to roll in from residents, family members, nursing home staffers, and vendors hired to provide services, it became clear he had no intention of doing so.

These complaints led to an investigation by the FBI's Atlanta office—in concert with the Department of Health and Human Services' Office of Inspector General and the Internal Revenue Service's Criminal Investigation. Evidence gathered by investigators and later introduced at trial showed that the services Houser provided to residents were so deficient that the judge determined them "worthless." It was a precedent-setting case...the first time ever that a defendant was federally convicted at trial for submitting payment claims for worthless services.

**There were other deficiencies in the homes as well, including:**

- **Inadequate staffing:** Houser failed to maintain a nursing staff sufficient to take proper care of the residents. Staffing shortages started plaguing the homes after Houser began writing bad checks to his employees, causing many to resign. He also withheld



**One of the dilapidated nursing homes owned and operated by a Georgia man recently convicted of Medicare/Medicaid fraud.**

health insurance premiums from his employees but let insurance lapse for non-payment, leaving many with large unpaid medical bills.

- **Failure to pay vendors:** Houser didn't pay food suppliers or providers of pharmacy and clinical laboratory services, medical waste disposal, trash disposal, and nursing supplies. Kind-hearted employees often used their own money to buy milk, bread, and other groceries so residents would not starve. They also brought in their own nursing and cleaning supplies and washed residents' laundry in commercial laundromats or even in their own homes.

And while his residents and employees were suffering, what were Houser and his wife doing? Spending their ill-gotten Medicare and Medicaid payments on hotel real estate investments, new homes, vacations, luxury cars, new furniture, and nannies for their child. Houser even gave money to an ex-wife...paying her a nursing home salary (even though she never worked there) and buying her a million-dollar home in Atlanta.

Said Atlanta Special Agent in Charge Brian Lamkin, "The level of greed and lack of compassion for others that was seen in this case reflect the very reason why the FBI, in working with its many and varied law enforcement partners, dedicates vast investigative resources to combating health care fraud."

And in this case, we were especially happy to see that all three nursing homes were eventually shut down by the state, and residents were moved into better living quarters to receive the care and compassion they deserve.





Left: Adam Mayes, our newest Top Ten fugitive, has been charged with murder, kidnapping, and unlawful flight to avoid prosecution.

## New Top Ten Fugitive

### Help Us Find Adam Mayes

*05/10/12 Update: Adam Mayes has died. The two sisters he allegedly kidnapped were found alive.*

Adam Mayes, wanted in connection with the recent kidnapping of a mother and her three daughters in Tennessee, has been added to the FBI's Ten Most Wanted Fugitives list. Bodies of two of the kidnap victims were found last week, but two girls—ages 8 and 12—remain missing and are considered to be in extreme danger.

**We need your help.** The FBI is offering a reward of up to \$100,000 for information leading directly to the arrest of the 35-year-old Mayes, who has been charged with murder, kidnapping, and unlawful flight to avoid prosecution.

On April 27, Jo Ann Bain, 31, and her three children were reported missing from Whiteville, Tennessee, and their vehicle was later found abandoned. Last week, authorities found the bodies of Bain and her oldest daughter, 14-year-old Adrienne, buried behind a mobile home where the Mayes family lived in Guntown, Mississippi.

"We believe Mayes could be anywhere in the United States, and we are extremely concerned for the safety of the girls," said Aaron Ford, special agent in charge of our Memphis office. "Anyone who has any information about this case, or if you've seen Mayes or the girls, please contact your nearest FBI office or the local police immediately."

**Mayes was last seen on May 1 in Guntown.** He has brown hair and blue eyes, is 6'3" tall, and weighs between 175 and 235 pounds. He may have changed his appearance by growing a beard or cutting his hair, and he may have changed the appearances of Alexandria and Kyliyah Bain as well. Mayes has connections in Mississippi,

Arizona, Texas, North Carolina, South Carolina, and Florida. He is considered armed and dangerous.

During a press conference today in Mississippi to announce Mayes' addition to the Top Ten list, Ford praised the "tireless efforts" of the local and state law enforcement officers and prosecutors from Tennessee and Mississippi who have worked around the clock on the case. "We are enlisting every available resource we have to locate the missing girls and to arrest Adam Mayes," he said.

Mayes is the 496th person to be named to the Ten Most Wanted Fugitives list. Since its creation in 1950, 465 fugitives on the list have been apprehended or located—153 of them as a result of citizen cooperation.

By adding Mayes to the list, Ford noted, "We are enlisting one of our most powerful weapons against crime—you, the citizens we serve. So as we continue our relentless search, we're asking for your assistance, too."

"It is law enforcement's responsibility to protect those who cannot protect themselves, and in this situation that is Alexandria and Kyliyah Bain," said Mark Gwyn, director of the Tennessee Bureau of Investigation. "These two children have lost their mother and older sister and deserve to be safely returned to their father. We believe someone out there knows where Adam Mayes and the girls are and will do the right thing and contact authorities with that information. It only takes one phone call."

# Economic Espionage

## How to Spot a Possible Insider Threat

This past February, five individuals and five companies were charged with economic espionage and theft of trade secrets in connection with their roles in a long-running effort to obtain information for the benefit of companies controlled by the government of the People's Republic of China.

According to the superseding indictment, the PRC government was after information on chloride-route titanium dioxide (TiO<sub>2</sub>) production capabilities. TiO<sub>2</sub> is a commercially valuable white pigment used to color paints, plastics, and paper. DuPont, a company based in Wilmington, Delaware, invented the chloride-route process for manufacturing TiO<sub>2</sub> and invested heavily in research and development to improve the process over the years. In 2011, the company reported that its TiO<sub>2</sub> trade secrets had been stolen.

Among the individuals charged in the case? Two long-time DuPont employees...one of whom pled guilty in fairly short order.

**Foreign economic espionage against the U.S. is a significant and growing threat to our country's economic health and security...and so is the threat from corporate insiders willing to carry it out.**

And because we're now in the digital age, insiders—who not so many years ago had to photocopy and smuggle mountains of documents out of their offices—can now share documents via e-mail or download them electronically on easy-to-hide portable devices.

**Why do insiders do it?** Lots of reasons, including greed or financial need, unhappiness at work, allegiance to another company or another country, vulnerability to blackmail, the promise of a better job, and/or drug or alcohol abuse.

**How to stop them?** Obviously, a strong organizational emphasis on personnel and computer security is key, and the FBI conducts outreach efforts with industry partners—like InfraGard—that offer a variety of security and counterintelligence training sessions, awareness seminars, and information.

**You can help as well.** In our experience, those who purloin trade secrets and other sensitive information from their own companies to sell overseas often exhibit certain



This digital billboard is being displayed in several regions of the country to raise awareness of the high cost of economic espionage.

behaviors that co-workers could have picked up on ahead of time, possibly preventing the information breaches in the first place. Many co-workers came forward only after the criminal was arrested. Had they reported those suspicions earlier, the company's secrets may have been kept safe.

Here are some warning signs that *could* indicate that employees are spying and/or stealing secrets from their company:

- They work odd hours without authorization.
- Without need or authorization, they take proprietary or other information home in hard copy form and/or on thumb drives, computer disks, or e-mail.
- They unnecessarily copy material, especially if it's proprietary or classified.
- They disregard company policies about installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential material.
- They take short trips to foreign countries for unexplained reasons.
- They engage in suspicious personal contacts with competitors, business partners, or other unauthorized individuals.
- They buy things they can't afford.
- They are overwhelmed by life crises or career disappointments.
- They are concerned about being investigated, leaving traps to detect searches of their home or office or looking for listening devices or cameras.

If you suspect someone in your office may be committing economic espionage, report it to your corporate security officer and to your local FBI office, or submit a tip online at <https://tips.fbi.gov/>.



Left: FBI Director Robert S. Mueller holds a candle during the dedication of names of fallen officers May 13 at the National Law Enforcement Officers Memorial. With him were (from left) Rep. Steny Hoyer; Linda Moon, national president of Concerns for Police Survivors; and Attorney General Eric Holder.

## Police Week

### FBI Honors Law Enforcement's Sacrifices

In 1962, President John F. Kennedy designated May 15 as Peace Officers Memorial Day and the week in which it falls as National Police Week. This year, as thousands of law enforcement officers from around the world gather in Washington, D.C. to honor colleagues who have made the ultimate sacrifice, the FBI joins with the rest of the country in paying tribute as well.

The week's events began Sunday evening with a candlelight vigil held at the National Law Enforcement Officers Memorial. The names of 362 fallen officers were read aloud, to be added to the nearly 20,000 other names permanently etched into the memorial's walls. The event was underscored by a preliminary report issued today that showed 72 law enforcement officers in the U.S. and Puerto Rico were feloniously killed in the line of duty in 2011; 50 were killed accidentally. The FBI will release final statistics this fall in the Uniform Crime Reporting (UCR) program's publication *Law Enforcement Officers Killed and Assaulted*, 2011.

"These men and women place the safety and security of others above their own," Attorney General Eric Holder said in remarks delivered at Sunday's ceremony. "When facing uncertain dangers and confronting unpredictable threats, they consistently respond with courage, selflessness, and strength. And every day—in communities nationwide—their contributions are felt and deeply appreciated."

Today, FBI Director Robert S. Mueller issued a video message recognizing officers for putting their lives on the line every day. "The FBI is proud to stand shoulder to shoulder with our law enforcement colleagues as we

continue our work together to protect our families and our communities," he said.

Also today, Director Mueller presided over a memorial service at FBI Headquarters to honor those lost from the FBI family, including two agents who passed away last year. Among the attendees were former FBI Directors Louis Freeh, William Sessions, and William Webster. Mueller said fallen officers and agents leave behind an enduring legacy and through their sacrifice set a standard for which we are forever grateful.

"Though their stories are different, they shared much in common," Mueller said. "They shared a devotion to service—service to the FBI, service to their communities, and service to our country. They shared a commitment to justice and to the rule of law. And they shared remarkable bravery."



Officers from around the country participate in the Police Unity Tour, a multi-day bike ride to raise awareness of the sacrifices made by law enforcement. The event also raises funds for the National Law Enforcement Officers Memorial.



# Celebrating Women Special Agents

## Part 1: May 12, 1972—A New Chapter is Opened

On a beautiful spring day in May—40 years ago this past weekend—FBI Acting Director L. Patrick Gray announced that “women applicants will now be considered for the FBI special agent position.” He noted that all other...

“...existing requirements for the special agent position will remain unchanged...the intensive 14-week special agent training course would remain unchanged [including] the use of .38 caliber revolver, shotgun, and rifle and a comprehensive physical fitness program.”

The FBI had long held that women couldn’t handle the physical rigors of the special agent position, which includes making arrests, taking part in raids, and engaging in self-defense. In those days, the Bureau operated under certain exemptions to federal regulations concerning equal employment. But times were changing—women were taking on more and more demanding positions, physically and otherwise.

With Hoover’s death on May 2, there was an opportunity to put into place changes that had been brewing for some time. So with the stroke of a pen, L. Patrick Gray opened a new chapter in FBI history.

### 40 Years of Firsts

On July 17, 1972, Joanne Pierce (Misko) and Susan Roley (Malone) were sworn in as FBI special agents and began that arduous training outlined in Gray’s press release, graduating in October. By the end of that year, 11 women would be sworn in.

In 1978, Special Agent Christine Karpoch (Jung) would become the first female firearms instructor—and she would shoot the coveted “possible,” a perfect score on the FBI’s Practical Pistol Range.

In 1985, Robin Ahrens became, tragically, the first female agent killed in the line of duty.

In 1990, Special Agents Susan Sprengel and Helen Bachor were sent to London and Montevideo, Uruguay to serve as the FBI’s first female assistant legal attachés.



The FBI Academy in 1972, when the first women in the modern era were sworn in as special agents.

In 1992, Special Agent Julianne Slifco became our first woman legal attaché, heading our overseas office in Vienna. And Birdie Pasenelli became our first female special agent in charge, overseeing the Anchorage Field Office. She later became the first woman assistant director at Headquarters, in charge of the Finance Division.

In 2001, Special Agent Kathleen McChesney became the first woman to attain the rank of executive assistant director, further chipping away at the glass ceiling.

Today, we have 2,675 women special agents, serving on and leading counterterrorism squads, cyber squads, counterintelligence squads, and criminal squads. They head field offices, including the largest in the Bureau—New York. They work as firearm instructors and in all other specialty fields. They lead Headquarters divisions and overseas offices. They are superb agents who just happen to be women.

### Wait a minute—weren’t there women agents in the 1920s?

Yes! When J. Edgar Hoover took over the Bureau in 1924, he inherited two female agents: Jessie B. Duckstein and Alaska P. Davidson, who both resigned within a few months as part of the Bureau’s reduction of force. But on November 6, 1924, Hoover himself changed the employment status of Lenore Houston from “special employee” in the New York office to “special agent.” She served in two other offices before resigning at the end of 1928. The next women agents weren’t hired until 1972.

*Part 2: Two women blaze a trail (page 59)*



**Left: FBI Director Robert S. Mueller speaks during a ceremony honoring Giovanni Falcone at FBI Headquarters.**

## Remembering Giovanni Falcone

### Italian Judge Assassinated by the Mafia 20 Years Ago

On May 23, 1992, Mafia hit men detonated a roadside bomb that killed Giovanni Falcone, his wife, and three bodyguards as they drove near Palermo, Italy. The assassination was payback for all the organized criminals Falcone had put behind bars as a prosecutor and judge.

**To mark the 20th anniversary of his murder, a tribute was held at FBI Headquarters to remember Falcone as a courageous opponent of the Mafia—and one of the earliest advocates of international cooperation in the fight against organized crime.**

Director Robert S. Mueller, who was joined by two former FBI Directors and several Italian dignitaries in paying tribute to Falcone, noted, “Long before ‘globalization’ became part of our vernacular, Judge Falcone recognized that no one department or country could fight crime alone. He went to great lengths to cultivate strong relationships—friendships—with partners here in the United States and around the world.”

The FBI’s special relationship with Falcone was forged decades ago through two major cases in the U.S. and Italy at a time when the Mafia was powerful in both places. Louis Freeh, a federal prosecutor in New York City who would later become Director of the FBI, was cracking down on the Mafia. In a case known as the Pizza Connection, the FBI, the NYPD, and federal prosecutors teamed with Falcone and Italian authorities to bust an international heroin smuggling ring that laundered drug money through pizza parlors. The 1985 trial cemented

Freeh and Falcone’s personal and professional relationships. At the same time in Italy, Falcone was prosecuting his own Mafia trial—the Maxi Trial—which put hundreds of mafiosi behind bars.

Although the Mafia for years threatened Falcone and his family and assassinated his Italian colleagues, “he carried on,” said Michael Kortan, assistant director of the FBI’s Office of Public Affairs. “He was a champion of the rule of law.”

Freeh remembered that although Falcone’s life was under constant threat, he always felt safe in the U.S. surrounded by his American law enforcement colleagues. “He loved the FBI,” Freeh said, adding that the Mafia made a “serious miscalculation” by killing Falcone. Instead of intimidating the Italian police, they—and the FBI—“rallied to the investigation of his murder.”

**After Falcone’s assassination, then-FBI Director William Sessions introduced the idea of a Falcone Memorial Garden at the FBI Academy in Quantico, Virginia. Two years later, then-Director Freeh saw the plan through and dedicated a bronze memorial to Falcone at Quantico.**

Prosecutor Liliana Ferraro, a friend and colleague of Falcone who took his seat after his assassination, said, “The Italian police and the FBI continue to work closely together against common enemies. As they fight organized crime together, they still use many lessons from Falcone, such as the importance of international cooperation and the protection of key witnesses.”

She added that Falcone “believed in friendship, loyalty, justice, and cooperation. On those shared values, we have developed a strong partnership that has enabled our countries to fight with success against organized crime and terrorism.”

“Judge Falcone always understood that there was strength in numbers,” Mueller said, “and that defeating the Mafia would require true solidarity. Due to his foresight, we have dealt a devastating blow to organized criminal syndicates.”

The relationships that Falcone forged years ago between the Italian National Police and the FBI “have borne tremendous fruit in this age of international crime and terrorism,” Mueller added. “Those friendships have set the standard for global cooperation among law enforcement.”

## Domestic Threat

### White Supremacy Extremism

It was a gruesome and hateful crime—three men with white supremacist tattoos punching and kicking the face and body of an African-American man at a bus stop in Houston last summer simply because of the color of his skin. All three were recently convicted of the attack, following an investigation by the FBI and its partners.

**It's not an isolated case.** It seems like a throwback to a different era, but white supremacy—which sees whites as inherently superior to those of other races—still exists in America today. Having those kinds of beliefs is not against the law...as a matter of fact, it's protected by the First Amendment. But white supremacy becomes a crime—and for the FBI, a form of what we call extremism—when it is furthered through threatened or actual use of force or violence or other illegal activity.

**The Bureau has been investigating the criminal activities of white supremacy extremists like Ku Klux Klan members since as early as 1918.** Today's extremists are more challenging than ever. They're affiliated with a variety of white supremacy groups, and they can be motivated by any number of religious or political ideologies. We're also seeing more lone offenders and small, violent factions of larger groups at work, which makes detection of these crimes tougher.

White supremacy extremists specifically target racial, ethnic, and religious minorities; the federal government; and in some instances, even each other. Their tactics include assault, murder, threats and intimidation, and bombings. They also commit other kinds of crimes—like drug trafficking, bank and armored car robberies, and counterfeiting—to fund their hate-filled activities.

Over the years, the federal government has successfully charged white supremacy extremists using a number of federal statutes, including civil rights violations, racketeering, solicitation to commit crimes of violence, firearms violations, explosives violations, counterfeiting and forgery, and witness tampering.

**In recent months, the FBI has led or participated in several significant investigations involving violence or attempted violence by self-admitted white supremacists.** A few examples:

- In February 2012, an Arizona man was sentenced to federal prison after pleading guilty to possessing and transporting improvised explosive devices near the U.S.-Mexico border.



- In January 2012, the last of four Arkansas defendants charged with firebombing the home of an interracial couple was sentenced to federal prison.
- In December 2011, a Washington man was sentenced to 32 years in prison for attempting to bomb a Martin Luther King, Jr. Unity Day march in Spokane.
- In May 2010, an Oregon man pled guilty to mailing a hangman's noose to the home of the president of a local NAACP chapter in Ohio.

**Moving forward, we see three keys to turning back the ongoing scourge of white supremacy extremism:**

- Our increased emphasis on the lawful gathering, analyzing, and sharing of intelligence on current and emerging trends, tactics, and threats.
- Continued collaboration with our local, state, tribal, and federal partners, especially on our Joint Terrorism Task Forces around the nation.
- And most importantly, the support of Americans who find these types of crimes abhorrent and antithetical to our way of life.

If you have information on domestic terror threats of any kind, submit a tip at <https://tips.fbi.gov> or contact your local FBI field office.



## Looking for Our Children

National Missing Children's Day 2012



These are just a very few of the children who are far from home today.

Please take a minute to look at all the faces on our Kidnapping and Missing Persons webpage and see if you can identify Asha, Daniel, Sierra, or any of the other children listed there with their stories.

Also take a look at the faces of the children who have been kidnapped by a parent—Melissa Hinako Braden and the many other kids.

And we hope you'll visit our Crimes Against Children page to learn all you can about what a dangerous world it

can be for our kids...and our Resources for Parents page to learn how to protect them in today's world.

To further help keep kids safe, we are also launching a new version of our Child ID app for Android mobile phones today.

*Note: The children pictured here may have been located since the above information was posted on our website. Please check our Wanted by the FBI webpage for up-to-date information.*

# The Case of the Misbranded Drug

## Leads to Massive Fine and Penalties

Fake treatments and bogus billings are all too common in the mega-billion-dollar business of health care fraud. But there's another serious dimension to the problem, especially when it comes to the health and safety of the American people.

It's called misbranding, and it involves hawking the benefits of a prescription drug without government approval or even claiming the drug can do something it can't.

**A good case in point: the prescription pain killer Vioxx, which first hit the shelves in May 1999 after approval by the Food and Drug Administration (FDA).** The drug—manufactured by Merck, (now known as Merck, Sharpe, & Dohme)—was designed to treat osteoarthritis, acute pain, and dysmenorrhea (painful menstrual cramps).

The trouble began when Merck sales reps began claiming the drug could also treat rheumatoid arthritis. Under federal law, in order to change or add a new usage for an already-approved drug, companies must either amend their original applications or submit a new one...complete with information about clinical trials and proposed labeling. Merck did submit an amended application, but not until 2001, almost two years after the company had been marketing Vioxx as a treatment for rheumatoid arthritis. FDA did not approve that application until April 2002. So that meant that from May 1999 to April 2002, Merck was promoting and selling a misbranded drug—despite an FDA letter of warning issued in September 2001.

**At the same time, Merck representatives were making inaccurate, unsupported, or misleading statements about Vioxx's cardiovascular safety in order to boost the sales of the drug.** But in September 2004, Merck voluntarily pulled Vioxx from the market when a study was halted because of an increased risk of heart attacks and strokes in study patients taking Vioxx.

**Our investigation began in late 2004,** when our Boston office and the local U.S. Attorney's Office learned about possible illegal activity surrounding the promotion and marketing of Vioxx before it was taken off the market.



Health care fraud cases are typically labor intensive, and this one was no exception, involving the review of thousands of Merck documents and interviews of numerous Merck employees, field sales representatives, doctors, consultants, researchers, and others. The case was truly a team effort with partners including the Department of Health and Human Services, FDA, Veterans Administration, Office of Personnel Management, and the National Association of Medicaid Fraud Control Units.

**The multi-year investigation paid off in a massive way:** Last month, Merck was ordered to pay a criminal fine of \$321 million for introducing a misbranded drug into interstate commerce after pleading guilty late last year. In November 2011, Merck also entered into a civil agreement to pay \$628 million to resolve additional allegations regarding off-label marketing of Vioxx and false statements about the drug's cardiovascular safety.

**Together, that's nearly \$950 million in penalties that will be returned to federal and state health care programs, a significant windfall to taxpayers.**

**Another significant outcome:** Merck agreed to enter into a corporate integrity agreement with the Department of Health and Human Services' Office of Inspector General that will strengthen the system of reviews and oversight procedures imposed on the company.

It all goes to show that crime doesn't pay...or as Boston FBI Special Agent in Charge Richard DesLauriers says, "No corporation is immune from being held accountable for criminal and civil violations of the law."





Left: A special agent overlooks the Shiprock land formation on the Navajo Nation in New Mexico.

## Journey Through Indian Country

### Part 1: Fighting Crime on Tribal Lands

Driving along a dirt road on the Navajo Reservation in New Mexico recently, a rancher crested a ridge and noticed two animals intent on something in a nearby ditch. As he approached, one of the scavengers loped away—the other looked up, its mouth glistening with blood. The rancher guessed one of his sheep had been attacked, but he soon discovered something much different: the discarded body of a murder victim. It was going to be another busy day for our agents in Indian Country.

**By law, the FBI is responsible for investigating the most serious crimes within Indian Country—homicide, child sexual assault, and violence against women among them. The numbers of such offenses are striking: approximately one out of every four violent crimes prosecuted federally by the Department of Justice occurs on Indian reservations.**

Investigating crimes on native lands poses a unique challenge for FBI personnel and their law enforcement partners. Working in Indian Country, as we call it, often means operating in isolated, forbidding terrain where cultural differences abound. Some older Native American people, for example, do not speak English. Dwellings may lack electricity or running water. On many reservations there are few paved roads or marked streets. Agents might be called to a crime scene in the middle of the night 120 miles away and given these directions: “Go 10 miles off the main road, turn right at the pile of tires, and go up the hill.” In some areas, crime scenes are so remote that cell phones and police radios don’t work.

Investigators must also deal with the emotional strain of the work—the brutality and frequency of the crimes can take a toll.

“The work our people are doing on the reservations is truly front-line,” said Carol K.O. Lee, special agent in charge of our Albuquerque office. “Agents have to be independent and adaptable to get the job done, because even with the excellent help of our law enforcement partners like the Bureau of Indian Affairs, the territory is so vast you rarely have the resources you need.”

Nationwide, the FBI has investigative responsibilities for about 200 federally recognized Indian reservations. More than 100 agents in 19 of the Bureau’s 56 field offices work Indian Country matters full time—and we’ve represented federal law enforcement on tribal lands since the 1920s. In New Mexico, home to a portion of the Navajo Nation—the largest reservation in the country, occupying an area bigger than the state of West Virginia—agents investigate cases against a backdrop of majestic mesas and stark beauty.

The murdered man mentioned above was found eight miles from the nearest paved road, not far from the landmark Shiprock formation sacred to the Navajo people. “The victim went out drinking with a bunch of guys and ended up dead,” said Special Agent Mike Harrigan, who supervises an Indian Country squad. The body has been identified and the death has been ruled a homicide, Harrigan explained, and investigators are tracking down leads. He noted that if the rancher hadn’t happened by, or the body had been dumped a few feet further from the road, “there is a good chance the victim never would have been discovered. Unfortunately, killings like this are all too common in Indian Country.”

Despite the difficulties they face, the dedication and commitment of FBI personnel in Indian Country has helped make Native American communities safer, said Special Agent in Charge Lee. “We have a long way to go, but we are definitely making a difference.”

*Part 2: Making an impact on the reservation (page 48)*



Scan this QR code with your smartphone to watch one in a series of related videos, or visit <http://www.fbi.gov/news/videos/>.



# New Top Ten Fugitive

## Help Us Find a Rapist and Murderer

Fidel Urbina, the subject of a nationwide manhunt since 1999 in connection with two sexual assaults and murder, has been named to the Ten Most Wanted Fugitives list.

The former Chicago resident is wanted for allegedly beating and raping a woman in March 1998 and—seven months later, while free on bond—for beating, raping, and strangling a second Chicago woman to death. That woman's body was found in the trunk of a burned-out car.

"Fidel Urbina is wanted for his role in two brutal attacks directed against innocent victims," said Robert Grant, special agent in charge of our Chicago office. "These crimes have demonstrated his violent nature and the need to locate and apprehend him before he can strike again. We are hoping that the publicity associated with this case, along with the significant reward being offered, will lead to his arrest."

**We are offering a reward of up to \$100,000 for information leading directly to Urbina's arrest.** The fugitive, who is now 37 years old, is a Mexican national who is 6 feet tall and weighs approximately 170 pounds. He has black hair, brown eyes, and a noticeably pockmarked right cheek. He has been known to use numerous aliases, including the names Lorenzo Maes, Fernando Ramos, and Fidel Urbina Aguirre. Given the nature of the charges against him, Urbina should be considered armed and dangerous.

The search for Urbina is being coordinated by our Violent Crimes Task Force (VCTF) in Chicago, which includes FBI agents, detectives from the Chicago Police Department, and Cook County Sheriff's Office investigators.

Special Agent Pablo Araya, fugitive coordinator for the VCTF, believes Urbina is hiding somewhere in Mexico. "Wherever he is," Araya said, "my guess is that women are in danger there, because this guy has shown no remorse and isn't likely to change his ways. That's why we need to catch him."

A federal arrest warrant was issued for Urbina in 1999, and in 2006 a provisional arrest warrant was signed by a federal magistrate in Mexico. But despite law enforcement's best efforts—which have included the case being profiled nationally on *America's Most Wanted* and locally on *Chicago's Most Wanted* television shows—the fugitive remains at large.



**Fidel Urbina is wanted for allegedly beating and raping a woman in March 1998. Seven months later, while out on bond, he allegedly beat, raped, and killed a second woman.**

**We need your help.** If you have any information about Fidel Urbina, please call the Chicago FBI at (312) 421-6700 or your nearest law enforcement agency or U.S. Embassy or Consulate. You can also submit a tip online at <https://tips.fbi.gov>.

"He's been on the run for over 10 years," Araya said. "He may be hiding in Mexico thinking that he is safe, but our hope is that because of the Top Ten publicity, someone who knows him or who recognizes his picture will think about that \$100,000 reward and give us a call."

Urbina is the 497th person to be placed on the FBI's Ten Most Wanted Fugitives list. Since its creation in 1950, 466 fugitives on the list have been apprehended or located—154 of them as a result of citizen cooperation.



Scan this QR code with your smartphone to watch a related video, or visit <http://www.fbi.gov/news/videos/>.



**Left: Special Agent Mac McCaskill visits a home on the Tohajiilee Reservation, a satellite reservation of the Navajo Nation where many homes lack electricity and running water.**

## Journey Through Indian Country

### Part 2: Making an Impact on the Reservation

Snow swirled in New Mexico's high plains as Special Agent Mac McCaskill slowed his vehicle at the bottom of a hill on the Tohajiilee Reservation. He engaged the four-wheel drive before continuing slowly up the steep, bumpy track on his way to deliver a subpoena in a violent assault case.

McCaskill had driven an hour from Albuquerque on this 20-degree morning—typical of the distances that often separate agents from their cases in Indian Country—and now he was knocking on the door of a small wooden structure with one boarded-up window. On the hillside just beyond the dwelling sat a rusted trailer and an outhouse. A young woman holding an infant opened the door and told McCaskill the man he was looking for would be back later.

**“On the reservation you can’t just call someone because many people don’t have a phone,”** McCaskill said, explaining the challenges of investigating crimes in Indian Country. **“Sometimes the best way to get anything done is to knock on doors.”**

In the process of knocking on doors and talking to people, McCaskill and other agents working in Indian Country become not just law enforcement officers but advocates for justice and sometimes even role models.

A New Mexico native, McCaskill said his eyes were “wide open” when he took an assignment in Indian Country. “Still, it’s difficult to comprehend the conditions on the

reservations and the kinds of crime we see here,” he explained. “People are living in really difficult circumstances.”

In Tohajiilee, a satellite reservation that is part of the Navajo Nation, many homes lack electricity and running water, and social ills such as alcoholism are rampant. These issues, along with the fact that there are only a handful of tribal police officers assigned to patrol a sprawling area of more than 120 square miles, contribute to a serious crime problem.

“There are terrible crimes that happen on the reservations that go virtually unnoticed by the world outside,” McCaskill said. “If they happened anywhere else, in Denver or in Dallas, it would be front-page news for a week.”

**As a result, he said, “we are serving a community that isn’t used to getting much service.”** Perhaps it’s not surprising then that women beaten by boyfriends or spouses or children sexually assaulted by family members may believe a call to authorities will do little to help them.

McCaskill works hard to change that perception. He patiently explained to the young mother the importance of serving the subpoena—so that the witness will testify, which could help make sure the violent offender stays in jail and no longer poses a threat to the community.

“Our caseloads may be 75 percent sexual assaults against children,” McCaskill said later. “People ask me if it’s difficult emotionally to work these cases, and my answer is always, ‘How can you not work them?’ These are cases where on a very fundamental level you are able to make a difference in a victim’s life by taking an abuser out of the family. When I help a victim and get to know the family,” he added, “I may be one of the few positive influences that they’ve ever seen from outside the reservation.”

Stopping that cycle of violence on the reservation is “extremely rewarding,” McCaskill said. “We are helping people here.”

*Part 3: Murder on the Zuni Reservation (page 51)*

## Crimes Rates are Down

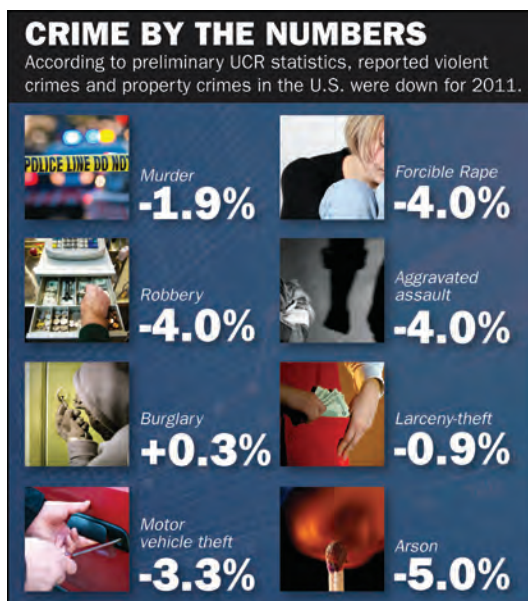
### According to 2011 Preliminary Report

Preliminary figures released today indicate that the number of violent crimes and property crimes reported by law enforcement across the nation during 2011 decreased when compared to 2010 figures.

According to our *Preliminary Annual Uniform Crime Report, January-December 2011*, violent crimes fell 4.0 percent, and property crimes dropped 0.8 percent. Arson—also a property crime even though its data is considered separately because of various levels of participation by reporting agencies—was down 5.0 percent overall.

#### Highlights from the preliminary report include:

- In the violent crime category, murder was down overall 1.9 percent from 2010 figures, while forcible rape, robbery, and aggravated assault all fell 4.0 percent.
- There was, however, an increase in murder in the Midwest (0.6 percent) and an 18.3 percent jump in murder in cities with populations of less than 10,000.
- In the property crime category, motor vehicle theft saw the largest decline (3.3 percent) from 2010 figures, followed by larceny-theft (0.9 percent).
- The only overall rise in property crimes was in the burglary category, which was up .03 percent overall, with increases of 3.2 percent in the Northeast, 1.3 percent in the Midwest, and 0.7 percent in the West.



This preliminary report includes four data tables. The first two tables show the percent change in offenses known to law enforcement for 2011 compared with those for 2010 by population group and region of the country, respectively. The third table reflects the percent change in offenses reported nationwide for consecutive years back to 2007. The fourth table presents the actual number of offenses known to law enforcement for agencies who provided 12 months of complete data and who serve a resident population of 100,000 or more.

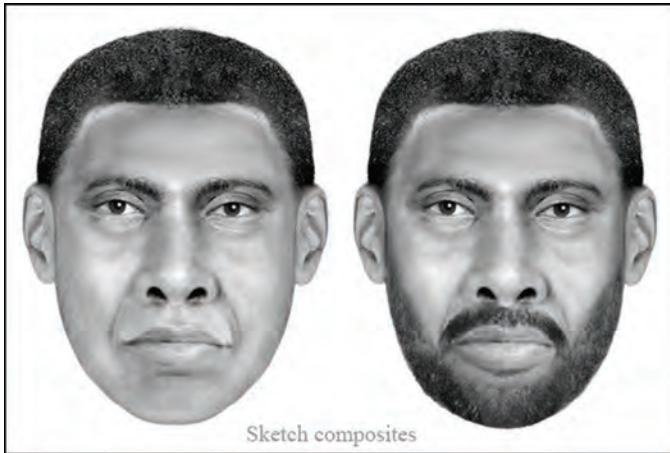
All of the final figures will be published this fall in *Crime in the United States, 2011*.

**Submitting Uniform Crime Reporting (UCR) data to the FBI is a collective effort on the part of city, county, state, tribal, and federal law enforcement agencies to present a nationwide view of crime.** Participating agencies voluntarily provide reports on crimes known to them, using uniform offense definitions. For the most part, agencies submit monthly crime reports to a centralized repository in their state. The state UCR program then forwards the data to the FBI's national UCR program, where staff members first review the information for accuracy and reasonableness, then enter it into the national UCR database.

The information is then publicly disseminated through various reports, including *Crime in the United States*, *Hate Crime Statistics*, and *Law Enforcement Officers Killed and Assaulted*, as well as through preliminary data reports and special reports on particular topics.

As always, the FBI cautions against drawing conclusions by making direct comparisons between cities or individual agencies—valid assessments are only possible with careful study and analysis of the unique conditions that affect each law enforcement jurisdiction.





## Help Us Catch a Killer

### Unknown Offender Linked by DNA in Two Separate Cases

On a Saturday night in October 2009, college student Morgan Harrington left a Metallica concert at the University of Virginia in Charlottesville and disappeared. It would be several months before her body was discovered in a field about 10 miles away.

**We need your help to find Harrington's killer.** The individual we are seeking has also been linked by DNA to a sexual assault in Fairfax City, Virginia, a suburb of Washington, D.C. Today, the Virginia State Police, Fairfax City Police, and the FBI released two enhanced sketches of the suspect and are reminding the public there is a reward of up to \$150,000 for information leading to an arrest and conviction in the Harrington case.

The multimedia campaign being launched today to draw attention to the investigation will include information on social media sites such as Twitter and Facebook, a public service announcement by Metallica, and electronic billboards in Virginia and along the East Coast.

"Bringing renewed attention to the case will get people thinking about it again," said Virginia State Police Special Agent Dino Cappuzzo. "Our hope is that someone will come forward and provide a crucial piece of information that will help us solve the murder."

Harrington was a 20-year-old student at Virginia Tech when she went to the concert that Saturday, October 17, at the John Paul Jones Arena on the University of Virginia campus. At about 8:30 p.m., she left the building and was unable to get back inside. She was last seen hitchhiking nearby.

**Left: A composite sketch of a suspect in a September 2005 sexual assault whose DNA is linked to Morgan Harrington's 2009 murder.**

Her remains were discovered the following January in a remote field on a farm in Albemarle County, Virginia. A camera she had that night and a distinctive Swarovski crystal necklace she was wearing have not been recovered.

FBI agents in our Charlottesville Resident Agency have been assisting state investigators, and profilers from our Behavioral Analysis Unit (BAU) have also provided consultation.

"A lot of BAU's work focused on the location of the body and what that told us about the offender," Cappuzzo said. "We believe he was intimately familiar with the farm and the surrounding area where the body was recovered. He may have been comfortable there and felt he was not at risk of getting caught."

**DNA recovered in the Harrington case was linked to an unknown offender in a September 2005 sexual assault in Fairfax City.** A 26-year-old woman was attacked at night while walking home from a grocery store. The offender was scared away by a passerby—but the victim got a good look at him, enabling a Fairfax City Police artist to produce a sketch of the attacker.

"It was a remarkable break to get the DNA match," said FBI Special Agent Jane Collins. The forensic evidence linked the two cases, so now we have a face to put with the suspect in the Harrington case. The suspect is described as an African-American male with black hair and facial hair (at the time of the 2005 attack). He is approximately 6 feet tall and was believed to be between the ages of 25 and 35 years old at the time of the Fairfax City assault.

**Help us catch Morgan Harrington's killer.** If you have any information about the Harrington case or the Fairfax City assault, contact the FBI at 1-800-CALL-FBI, the Virginia State Police Tip line at 434-352-3467, or submit a tip online at <https://tips.fbi.gov>.



Scan this QR code with your smartphone to watch one of three related videos, or visit <http://www.fbi.gov/news/videos/>.

# Journey Through Indian Country

## Part 3: Murder on the Zuni Reservation

Special Agent John Fortunato walked behind the abandoned house on the Zuni Reservation in western New Mexico and pointed out where Floyd Yuselew dug a grave to bury the friend he had murdered with an ax to the head.

The two had been drinking, and investigators believe the murder was committed because Yuselew thought his buddy had been flirting with his girlfriend. When tribal police and the FBI learned of the crime in March 2009, they found the victim still sitting in the chair where he had been killed months earlier. Because the house was unheated throughout the cold winter, the body—and the crime scene—had been perfectly preserved.

Uncertain what to do with the body, and not wishing to live in his house with a corpse, Yuselew and his girlfriend moved in with friends. Periodically, he returned to dig in the frozen backyard to make a grave. Later, Yuselew was afraid his girlfriend would turn him in for the murder when their relationship ended badly, so he called the Zuni police, told them about the body, and tried to pin the crime on her.

**As unusual as the case may seem, in many ways it is a common Indian Country crime: a tragic killing successfully investigated and prosecuted thanks to the strong relationships between tribal authorities, the FBI, and federal prosecutors.** Criminal jurisdiction in Indian Country is a complicated web of tribal, state, and federal rules. The sovereign status of many tribes precludes most states from exercising jurisdiction. Instead, that authority resides with the tribes, but only for non-felony offenses. It is the FBI's responsibility to investigate major crimes such as murder, and tribal authorities rely on the muscle of the federal judicial system to prosecute those crimes to the fullest.

"By law these major crimes are federally prosecuted, and the FBI is the vehicle for getting them to federal court," said Special Agent Mike Harrigan, who supervises a squad of Indian Country investigators. "But the successful investigation of such crimes isn't just a Bureau role," he added, "it is a tribal and Bureau partnership."



Floyd Yuselew killed his friend in this house on the Zuni Reservation during a confrontation after a night of drinking in 2009. The victim's body was found months later, still well-preserved by the winter freeze.

"We have a close relationship with all the tribal police," Fortunato said. "It would be difficult for us to do our jobs without that partnership, and they depend on us as well." In the Yuselew case, for example, Fortunato called in the Bureau's Evidence Response Team (ERT) to help work the crime scene.

"When ERT processed the scene," he explained, "there was a lot of blood and other evidence, like alcohol cans we were able to pull fingerprints from. The blood spatter and other evidence inside the house made it clear it was not the girlfriend who did the crime."

**In the end, Yuselew pled guilty to second-degree murder and is currently serving a 17-year sentence.**

The case is one of many senseless crimes Fortunato and his colleagues investigate in Indian Country. "We invariably see the bad side of things here," he said. "We are constantly seeing tragedy, loss, and people who hurt family members. That is the hardest thing for me about working in Indian Country."

Still, Fortunato is pleased that justice was served in the Yuselew case, and he believes in the goodness of the vast majority of Native Americans. "Anyone who has visited the Navajo and Zuni reservations and spent time here will tell you that most of the people are terrific, very friendly, and welcoming."

*Part 4: Teamwork makes a difficult job easier (page 52)*



## Journey Through Indian Country

### Part 4: Teamwork Makes a Difficult Job Easier

Louis St. Germaine, a long-time criminal investigator for the Navajo Nation, has worked closely with FBI agents over the years and recalls the surprise many of them express when first coming to Indian Country.

**“Sometimes agents expect to see street numbers and paved roads,” said St. Germaine, who was born and raised on the reservation. “Out here, you make one wrong turn at an isolated place and go a few hundred feet and you can get very lost very quickly.”**

“And when the sun goes down,” said Malcolm Leslie, another Navajo criminal investigator, “in some places on the reservation you can’t see your hand in front of your face.”

From the most basic task of finding a crime scene to more complicated matters regarding language and cultural barriers, FBI agents in Indian Country depend on their local, federal, and tribal law enforcement partners. And our partners rely equally on us—for expertise, training, and other resources.

“I don’t think one can do without the other,” said St. Germaine. “Navajo Nation investigators—we’ve been here a long time. We are familiar with the area, the crimes, and the people. The FBI is well-skilled in doing investigations. So we combine our talents, and it works well.”

St. Germaine was one of the original members of the first Safe Trails Task Force, which the FBI created

---

**Left: The uninitiated can get lost very quickly on the reservation. “When the sun goes down,” said a Navajo criminal investigator, “in some places on the reservation you can’t see your hand in front of your face.”**

---

in 1994 on the Navajo Reservation and has since expanded to 15 locations around the country. The idea is to unite the Bureau with other federal, local, and tribal law enforcement agencies to combat Indian Country crime.

Through the task force and other initiatives, the FBI provides invaluable training and equipment to tribal law enforcement. “It has helped us do our job,” St. Germaine said. “We are challenged financially on the Navajo Nation. The FBI supplies us with vehicles and other equipment. Without that contribution,” he added, “I think we would be in real serious trouble.”

“And without our tribal partners,” said Special Agent Lenny Johns, who supervises our Santa Fe Resident Agency, “it would be virtually impossible for the Bureau to accomplish its mission in Indian Country. Many times it’s just one FBI agent on the reservation dealing with a complex crime scene. The tribal criminal investigators and evidence technicians are critical to the process of conducting interviews and collecting evidence. Without them, we’d get very little traction.”

“The FBI brings resources that we’re in dire need of,” added veteran criminal investigator Leslie. “But they also bring knowledge.” Leslie has received a variety of FBI training, both in the classroom and on the job at crime scenes.

Donovan Becenti, a Navajo Nation crime scene technician, has processed many crime scenes with the FBI’s Evidence Response Team (ERT) and has benefited from FBI training as well.

“The partnership is great,” Becenti said. “ERT out of Albuquerque is where I’ve gotten most of my training. Without them, I wouldn’t be where I am today as far as my skill level. And they also provide equipment—evidence collection supplies and whatever else I need to help get the job done.”

Becenti was recently presented with an FBI Director’s Certificate for his many years of helping ERT process crime scenes on the Navajo reservation. “When you work alongside someone for 12 straight hours on a homicide scene in freezing fog and sub-zero temperatures,” he said, “it builds mutual trust and respect.”

*Part 5: A zero-tolerance approach (page 56)*



## Operation Cross Country

### Nationwide Sweep Recovers Child Victims of Prostitution

In the continuing effort to address the national problem of child sex trafficking, the FBI and our partners today announced the results of a three-day law enforcement action in which 79 child victims of prostitution were recovered and more than 100 pimps were arrested.

**Operation Cross Country VI**, part of the Bureau's **Innocence Lost National Initiative**, was conducted over the past 72 hours in 57 cities around the country with the help of state and local law enforcement and the National Center for Missing & Exploited Children (NCMEC).

"Child prostitution remains a major threat to children across America," said Kevin Perkins, acting executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch. "It is a violent and deplorable crime, and we are working with our partners to disrupt and put behind bars individuals and members of criminal enterprises who would sexually exploit children."

The Innocence Lost National Initiative was launched in 2003 by the FBI's Criminal Investigative Division in partnership with NCMEC and the Department of Justice's Child Exploitation and Obscenity Section.

To date, 47 Innocence Lost Task Forces and working groups have recovered more than 2,200 children from the streets. The investigations and subsequent 1,017 convictions of pimps, madams, and their associates who exploit children through prostitution have resulted in lengthy sentences—including multiple sentences of 25 years to life in prison—and the seizure of more than \$3 million in assets.

Operation Cross Country national sweeps usually grow out of local law enforcement actions—officers and other task force members target places of prostitution such as truck stops, casinos, street "tracks," and Internet websites. Initial arrests are often for violations of local and state laws relating to prostitution or solicitation. Intelligence gathered from those arrested can reveal organized efforts to prostitute women and children across many states. FBI agents further develop this information in partnership with U.S. Attorney's Offices and the Department of Justice's Child Exploitation and Obscenity Section to bring federal charges against pimps and other sex traffickers.



FBI and law enforcement personnel talk to a victim during the Operation Cross Country VI sweep.

**"It is clear that child prostitution and sex trafficking do not just occur somewhere else on the other side of the world," said Ernie Allen, president of NCMEC. "These insidious crimes are occurring in American cities, and the victims are American kids."**

At a press conference today at FBI Headquarters in Washington, D.C., Allen thanked the FBI for its leadership over the past decade in fighting domestic sex trafficking. The Bureau, in turn, expressed gratitude to the more than 8,500 local, state, and federal law enforcement officers representing 414 separate agencies who participated in the most recent Operation Cross Country and ongoing enforcement efforts.

In addition to its enforcement successes, the Innocence Lost National Initiative brings state and federal law enforcement agencies, prosecutors, and social service providers from across the country to NCMEC, where the groups receive training together.



Left: J. Edgar Hoover is seen in a George Washington University Law School yearbook picture from 1916.

## The Hoover Legacy, 40 Years After

### Part 2: His First Job and the FBI Files

J. Edgar Hoover was just 18 years old when he took his first job in government—an entry-level position as a messenger in the orders department of the Library of Congress.

**It was October 13, 1913. No one knew it at the time, but an important foundation in Hoover's future career as FBI Director (and in the Bureau itself) was being laid.**

Young Hoover excelled at his work. He impressed his supervisors and was awarded multiple raises. His position in the orders department—which acquired books, manuscripts, and other items for the Library's collections—included working in the cataloging department and the loan division. The Library was a half-mile from his house and allowed him to attend law school at night, where he was studying hard and learning quickly.

On July 25, 1917, Hoover left the Library, and he took a job the next day as a clerk in the Department of Justice, where his story becomes better known.

**Hoover's experiences with the Library of Congress and its innovative organization of knowledge have often been credited with influencing the creation of the FBI's own knowledge management system—the FBI files.** The filing system he helped architect became almost legendary for its efficiency and over the years has been fodder for books, news stories, movies, and even conspiracy theories of all sorts that exaggerate the size and scope of the files.

But were the FBI files modeled on the Library of Congress system? Actually, no. The FBI filing system is based on the type of case the file covers. Each file is designated by a classification number—for example, kidnapping cases begin with the number 7, espionage cases with the number 65. This is only vaguely similar to the Library's system. Also, these classifications were already being used by the Department of Justice; Hoover's Bureau simply adapted them for its own purposes.

**What is true, however, is that Hoover's Library experience did have a significant impact on how the FBI's filing system was used and adapted.** In a 1951 letter referencing his former position, Hoover wrote, “[T]his job ...trained me in the value of collating material. It gave me an excellent foundation for my work in the FBI where it has been necessary to collate information and evidence.”

This ability to synthesize information was key. In 1921, as assistant director, Hoover oversaw the reform of the Bureau's files, which were in disarray after several organizational restructurings. For the reform, Hoover took something old—the Department of Justice system—and something new—indexing the files as they were created. And then he used something borrowed—from the Library of Congress: the idea of extensive cross-references within the card indices that provided access to the content of the FBI files. Each cross-reference pointed back to the original file and allowed for comparison of information across all files. So an agent or clerk could find a person's name, an event, a location, or any number of other things, even if it was spread across dozens of different files at Headquarters and in the field offices. In a profession that requires intelligence at its fingertips and the ability to know everything that's available, this system was crucial to the success of Hoover's Bureau as it grew and adapted to its expanding mission.

In the end, Hoover's work at the Library helped the Bureau to create a filing system that—in comparison to others of the day—was “unique unto itself,” as one records manager noted in 1941 when surveying the state of records across the nation.

*Part 3: Another side of Hoover (page 62)*

# Inside the Denver JTTF

## Part 1: Vigilance Against Terrorism

It was September 2009—a few days before the eighth anniversary of the 9/11 attacks—when the Denver Joint Terrorism Task Force (JTTF) received word that a Colorado resident and al Qaeda recruit was about to carry out a major terrorist attack. The jihadist needed to be located with the utmost urgency.

**“We got the call on Labor Day,” recalled Special Agent John Scata, who supervises one of Denver’s two international terrorism squads, “and we immediately began working around the clock.”**

Using the JTTF’s multi-agency approach to conducting investigations and gathering and sharing intelligence, task force members located Najibullah Zazi and helped track him to New York City, where he intended to become a suicide bomber in the subway system around the time of the 9/11 anniversary. “If we hadn’t found him in Denver as quickly as we did,” Scata said, “he might have gone into the wind and things could have turned out differently.”

Zazi and two of his high school classmates had previously traveled to Pakistan to receive al Qaeda training, including how to make bombs. His self-described plot to “weaken America” by killing innocent subway riders has been characterized as one of the most serious terrorist threats to the U.S. since the 9/11 attacks.

“Zazi is part of the spread of homegrown violent extremism in America,” said James Yacone, special agent in charge of our Denver office. “He was trained internationally but he became radicalized in the U.S. through the Internet. He was planning and facilitating his attack in Colorado, but his target was New York City.”

**The plot was foiled thanks to an all-out effort by law enforcement and intelligence agencies around the world. Much of that effort was focused through Denver’s JTTF, which is comprised of more than 20 local, state, and federal agencies.** There are actually three separate squads that form the task force—two that deal with international terrorism and one that concentrates on domestic terrorism.

Created in 1994, Denver’s JTTF is one of the Bureau’s oldest (our New York office established the first in 1980). “Our task force is very active,” said Yacone. “The Zazi



James Yacone, special agent in charge of our Denver office, discusses the role of the Denver Joint Terrorism Task Force, or JTTF.

case was well publicized, but our squads handle many other counterterrorism investigations—international and domestic. Protecting the country from terror attacks is the FBI’s number one priority.”

The JTTF’s team concept works well, Yacone explained. “All the local and state police officers and detectives on the task force have the same clearances that our agents do. They sit side by side, work together, and have the same access to all our resources.” More than 100 FBI-led JTTFs located around the country are organized the same way.

John Nagengast, a detective with Colorado’s Aurora Police Department, is a JTTF task force officer who worked on the Zazi case. “I am basically a local cop who deals with local crime,” he said. “Working the Zazi case opened up my world to the threat of terrorism.”

Nagengast explained that “a lot of entities were involved in the investigation, including the military and the intelligence community—and the Denver JTTF was central to the operation. We were ground zero for the Zazi investigation.” He added, “I got to see very quickly how the Bureau, locals, and state law enforcement came together with agencies around the world to prevent this attack. It was amazing to be a part of it.”

*Part 2: Partners help cast a wide safety net (page 58)*





## Journey Through Indian Country

### Part 5: A Zero-Tolerance Approach

The arrest of a 20-year-old Zuni woman for selling two baggies of cocaine that each contained less than one gram of the drug might be considered a minor offense in many jurisdictions—but in Indian Country, federal prosecutors are taking a different approach.

**“We have zero tolerance for drug trafficking in Indian Country,”** said New Mexico U.S. Attorney **Ken Gonzales**. Because alcohol and drugs fuel serious crimes on the reservation, and because public safety is at stake, Gonzales sees the no-tolerance program as an important part of his office’s efforts to fight crime on the reservations.

“If you identify somebody in the community who has been causing problems for years and years, has rotated in and out of the criminal justice system, and is nevertheless out on the street causing big problems,” Gonzales said, “we will take that case if the individual is caught trafficking drugs, no matter what the amount. In most instances,” he explained, “we require a certain amount of drugs to be able to prosecute a case federally. But we’ve made it a priority in Indian Country to lower, if not eliminate, our thresholds to take these cases.”

The 20-year-old Zuni woman, who was recently sentenced to a year in prison for cocaine trafficking, “had a significant tribal court history and was clearly a problem in the community,” Gonzales said, which is why the FBI and the U.S. Attorney’s Office got involved. Ordinarily, our agents investigate major crimes in Indian Country. But going after habitual small-time drug offenders is another key way to make reservation communities safer.

Left: “We have zero tolerance for drug trafficking in Indian Country,” said U.S. Attorney Ken Gonzales. “We’ve made it a priority...to lower, if not eliminate, our thresholds to take these cases.”

“When you take even one of those bad actors out of the community, you’ve made a big impact,” said Special Agent Lenny Johns, who supervises our Santa Fe Resident Agency. “We have a very close working relationship with the U.S. Attorney’s Office on the no-tolerance program—and other programs—and we are very proud of the results of that partnership.”

“Having the FBI and federal prosecutors working in a side-by-side partnership to identify unique cases that impact the community—which we are finding to be gang cases and drug trafficking—and targeting those cases for fast-track investigation and prosecution has really made a difference,” Johns added.

Coupled with other initiatives such as the Tribal Law Enforcement Act—passed by Congress in 2010 to strengthen law enforcement on the reservations and enable tribal courts to hand down stiffer sentences—Johns and Gonzales believe the federal justice system is making an impact in Indian Country, even though they acknowledge there are many challenges.



U.S. Attorney  
Kenneth Gonzales

“The Department of Justice can do a lot to prosecute crime,” Gonzales said. “With the help of the FBI, the Bureau of Indian Affairs, and our local tribal law enforcement partners, we can investigate and take troublesome people out of the community for extended periods of time. In that way, we are also doing a lot to prevent crime. It’s all part of our overall anti-violence strategy.”

“There is no question that a serious crime problem exists in Indian Country,” Johns said.

“The bottom line in all our efforts,” he added, “is that we are dedicated to making sure that innocent people on the reservation are not victimized.”

*Part 6: Invaluable experience on the reservation (page 60)*

# If It's Too Good to Be True...

## Massive Ponzi Scheme Proves Age-Old Adage

If a respected member of your community offered you an investment opportunity, you might consider it. Especially if it's a man of the cloth.

For nearly a decade, Martin Sigillito—a bishop in the American Anglican Convocation and a St. Louis attorney—convinced 200-plus people to do more than just consider it: they actually entrusted him with their money to invest in a financial venture. But this venture turned out to be an old-fashioned Ponzi scheme, and in April of this year, Sigillito was convicted of leading a conspiracy that swindled \$52 million from victim investors.

**How the scam began.** In late 2000, Sigillito opened a law office but didn't actually practice law—instead, he advertised his “international business consulting services.” One of the “services” he offered was participation in the British Lending Program (BLP), transformed by Sigillito into a Ponzi scheme. Through the BLP, investors could “loan” money to a real estate developer in the United Kingdom for short periods of time, mostly one year, at high rates of return—between 10 and 48 percent.

This real estate developer, according to Sigillito, had a knack for spotting undervalued properties he could flip for a profit, had options on land that would become valuable when re-zoned, and had inside connections with British authorities. It sounded like a win-win for investors.

Unfortunately, this British developer was not the wunder-kind Sigillito made him out to be—he was just another link in the criminal conspiracy.

**How did Sigillito convince his investors to part with their money?** He exploited his personal ties to people and particular groups he was affiliated with—like his church, social clubs, professional acquaintances, family, and neighbors—in a technique known as affinity fraud. He also held himself up as an expert in international law and finance and claimed he was a lecturer at Oxford University in England (when in reality he had simply taken part in a summer legal program at Oxford).

Sigillito, who also conspired with another American attorney, insisted that his investors' funds initially be placed into his trust account, from which he would



One of the United Kingdom hotel properties that victims of Martin Sigillito's Ponzi scheme thought they were investing in.

take exorbitant fees for himself and his co-conspirators. Even though he told investors he would then transmit the money to the U.K., Sigillito actually kept most of the funds in one or more American bank accounts he controlled.

**For a while, the scam was self-sustaining:** Many investors let their interest payments accrue and rolled their loans over every year, plus Sigillito brought in enough new investors to make interest and principal payments to any previous investor who asked for payment. And all the while, he made enough in “fees” to support his affluent lifestyle, which included exclusive club memberships, expensive vacations, a country home, a chauffeur, private school for his kids, and collections of rare and antique books, maps, prints, coins, jewelry, and liquor.

**How the scam ended.** Eventually, an increasing number of investors meant increasing payout requirements, which resulted in the BLP making late interest payments or missing interest payments all together. Then investors began clamoring to withdraw their funds. And finally, Sigillito's own assistant became suspicious of his activities and contacted the FBI.

The takeaway from this case? Fully investigate any investment opportunity before handing over your hard-earned money.



Left: Steve Garcia, a major in the Colorado State Patrol who oversees the Colorado Information Analysis Center, or fusion center, in Denver.

## Inside the Denver JTTF

### Part 2: Partners Help Cast a Wide Safety Net

The more than 100 FBI-led Joint Terrorism Task Forces (JTTFs) around the country rely on a network of local, state, and federal partners to help protect the nation. In Denver, one of our key partners is the Colorado Information Analysis Center.

Known by its acronym, CIAC—pronounced “kayak”—was established by the state legislature in the wake of the 9/11 attacks to bring organizations together to gather, analyze, and share information. Working in tandem with the JTTF, the CIAC’s multi-agency fusion approach casts a wide security net throughout the Colorado region.

**“We have representatives from the FBI, the Department of Homeland Security, local law enforcement, local emergency managers, and local firefighters who all come together to share information,” said Steve Garcia, a major in the Colorado State Patrol who oversees the center’s operations. “That information is fused—hence the term fusion center—to create an intelligence-sharing environment.”**

The FBI is the fusion center’s investigative arm “and the single most important partner we have,” Garcia added, explaining how the two organizations work hand in hand. “Last year we received over 400 tips and leads that came in to our website or 1-800 number regarding suspicious activity. The FBI, being the primary agency for counter-terrorism, goes out and investigates those leads.”

“Our relationship with the fusion center is as significant as any relationship we have,” said Steve Olson, an assistant special agent in charge in our Denver office who

supervises the JTTF. He explained that the fusion center not only provides tips and leads, it helps fill intelligence gaps.

In the Zazi case (see page 55), investigators needed to find out where Zazi had acquired bomb-making chemicals. The fusion center’s 650 terrorism liaison officers (TLOs)—consisting of local sheriff, police, and fire department personnel—fanned out in their jurisdictions to canvass beauty and farm supply stores where those chemicals might have been purchased.

**“We sent out a request for information through our TLO network,” Garcia said, “and they were able to talk to local merchants to see if Zazi had been there to buy the precursors to TATP, which is what he was eventually found guilty of.”**

“The TLOs are a significant force multiplier for us,” Olson noted. “They can reach parts of the state that we can’t readily access.” In addition to gathering intelligence, the TLOs can also be tasked with disseminating information. By alerting local merchants that terrorists might be seeking certain kinds of chemicals, for example, law enforcement can set tripwires so merchants will report suspicious activity.

“If somebody comes in your store that you don’t recognize and requests a large amount of a precursor chemical, we want you to reach out to your local authorities,” Olson said. “That tip makes it to the fusion center through a TLO, and then it comes to the JTTF for further investigation. That allows us to stay one step ahead of potential problems.”

The FBI maintains a full-time intelligence analyst at the fusion center, which facilitates the immediate sharing of information. “Our motto at the CIAC is that information sharing is a contact sport,” Garcia said. “You’ve got to get up and talk to someone and share that information rather than just sending an e-mail. It’s important to have that day-to-day, face-to-face contact.”

*Part 3: The JTTF’s WMD coordinator (page 63)*



# Celebrating Women Special Agents

## Part 2: Two Women Blaze a Trail in 1972

They were known as the nun and the Marine. The respective backgrounds of Joanne Pierce Misko and Susan Roley Malone could not have been more dissimilar. But 40 years ago, on July 17, 1972, the two women were drawn together by a shared goal—to become FBI special agents.

Up until then, under the leadership of longtime FBI Director J. Edgar Hoover, only men could be agents. But just weeks after Hoover died in May 1972, the Bureau's acting director—motivated in part by new equal rights laws—changed the men-only policy that had been in place since the Prohibition Era. So on a balmy Monday exactly four decades ago, the two women assembled with 43 similarly pressed and starched men at FBI Headquarters to take their oath before heading down to the FBI Training Academy in Quantico, Virginia for 14 weeks (now 20) of physical and mental conditioning.

**The new agent training was tough enough on its own—firearms, strength, endurance, self-defense, academics. But for Misko and Malone, who were expected to meet the requirements long in place for males, there was the added dimension of their novelty, which was not universally embraced at first.**

"I'm sure when they first saw that there were two women in their class it was like, 'Oh, we got them,'" Misko recalled in a recent interview. Malone, who had already broken some stereotypes as a Marine, remembers a fellow classmate confronting her during a break, brusquely asking why she thought she could be an FBI agent. "And I sat down and I talked to him," Malone stated. "I said, 'I love my country just like you do. I want to be here for the same reasons that you want to be here.'" He heard her out. And in the weeks that followed, the two women set out to demonstrate that they belonged in their coveted slots in New Agent Class 73-1. They won over some of the most ardent doubters by rising to every challenge and helping their classmates over some hurdles along the way.

**"We got along pretty well and everybody kind of pulled together as a class,"** said Misko, who was 31 at the time. "Because in training I think we were all in the same boat. We were all trying to prove ourselves."

Permitting women into the ranks of special agents was a big story at the time, but the Bureau tried to minimize



**Joanne Pierce Misko, in red and lower right, and Susan Roley Malone, seen at the FBI Training Academy in 1972 and today, were the first women of the modern era to become special agents.**

distractions in order to maintain the integrity of training. "They wanted us to be like any other agent," said Malone, who was 25 when she entered the FBI Academy. "They didn't want to make this inordinately special or set us apart from our fellow agents. I think that was very important at the time. We wanted to be just another agent."

**Despite following wildly divergent paths to Quantico and having very little in common, Misko and Malone—the nun and the Marine—leaned on each other to get through training.** "We supported each other," said Malone. "We were complementary. We worked together. We would practice the run at night, we would go to the gym and work out. We were allies. There's that bond there when you're someone's roommate and you're going through the same training. That's a lifelong bond."

**Misko and Malone completed the training in October 1972** and, like all new agents, received orders to report to one of the Bureau's field offices. Malone was sent to Omaha and Misko to St. Louis. Both women recall being met with some initial resistance in the ranks, but quickly showed they could pull their weight. The former roommates would cross paths occasionally in their successful careers. They recognize today they were trailblazers, but that was never their goal.

"I honestly didn't see myself as a pioneer," said Misko, now 71. "It was just a role that I was fortunate enough to become a part of."

Malone, 65, echoed Misko's comments. "I was an agent first and Joanne was an agent first. We wanted to be agents first. We just happened to be women."

*Part 3: Early pioneers tell their stories (page 64)*



**Left: For agents, the unique experience of working Indian Country crimes includes deploying—often by themselves—to remote sites within pueblos or reservations.**

## Journey Through Indian Country

### Part 6: Gaining Invaluable Experience on the Reservation

It wasn't long after his arrival in Indian Country that Special Agent John Fortunato started carrying dog biscuits in his FBI vehicle. Some of the wild dogs who roam the New Mexico reservations are a lot easier to befriend or distract when they are offered food.

**That's just one small example of how investigating crimes in Indian Country makes agents resourceful—and provides them with an intensive professional experience they may not get anywhere else in the FBI.** “We like to say that six months as an investigator on the reservation is like two years at any other Bureau office,” Fortunato said. “That's mainly because of the nature of the crimes here and our jurisdictional responsibilities.”

Since 9/11, the FBI has become an intelligence-based, threat-driven organization. Regarding terrorism, for example, the mission is to prevent acts of terror rather than investigate them after they occur. “But in Indian Country,” said Special Agent Lenny Johns, who supervises our Santa Fe Resident Agency, “the majority of the crimes we have jurisdiction over are still very reactive for us.”

That means when the FBI is called to the reservation, usually a serious crime has already been committed. “Our agents, and particularly new agents,” said Johns, “get a ton of experience in Indian Country they can apply in other programs later in their careers. That experience includes deploying—often by themselves—to a remote site within a pueblo or reservation, dealing with folks that have a different cultural background than they do, and success-

fully navigating that environment to conduct interviews, follow up on leads, collect evidence from a crime scene, and build a prosecutable case for the U.S. Attorney's Office.”

“The sheer number of cases we're handling adds to the training experience,” said Fortunato, who worked in our New York Field Office on counterintelligence matters before coming to Indian Country several years ago. His counterintelligence cases spanned months and even years. “Here,” he explained, “because we are reacting to crimes, we investigate an assault or homicide with our tribal partners, and often within a matter of days we are making an arrest.”

And where he had only a handful of cases in New York, Fortunato—and most of the agents working in New Mexico's Indian Country—have anywhere from 30 to 50 cases to work at any given time. And they are all major crimes such as murder and child sexual assault.

**“It's a 24-7 job,” noted Special Agent Mike Harrigan, who supervises an Indian Country squad.** “An agent is always on call. If something happens, even in the middle of the night and the crime scene is two hours away by car, the on-call agent responds from home. That's how it works in Indian Country.”

“The agents and professional staff working here in Indian Country are as dedicated as any group I have served with during my 25 years in the FBI,” said Carol K.O. Lee, special agent in charge of our Albuquerque office. “They really care about the people on the reservations and making those communities the best and safest places they can be.”

## ‘Play How You Practice’ FBI’s WMD Training Workshop Tests Massive Response

On May 18, a carrier ship bound for the Port of New Orleans left a Caribbean nation weighted with 12,000 tons of ammonium nitrate. Intelligence later revealed that two of the ship’s crew members were on terrorist watch lists. Meanwhile, a few miles outside New Orleans, police received a report of someone suspiciously circling a chemical plant in a car while taking pictures.

What may have appeared at first to be isolated incidents were actually parts of an elaborate drill to test how well local, state, federal, and even international emergency responders would coordinate and communicate in the fog of an unfolding terror plot. The mock scenario, which played out in a day-long tabletop exercise in New Orleans last May, was a cascade of escalating disasters that involved the revelation of the plot, multiple shootings, a chemical leak, hostage-taking, and the release of nuclear radiation. The object of the exercise was to overwhelm the region’s elaborate web of responders and investigators and force them to turn a critical eye to how prepared they are for a real disaster involving weapons of mass destruction, or WMD.

**“We are training to identify what the WMD threat is around the critical infrastructures and around our key resources,”** said John Perren, assistant director of the FBI’s Weapons of Mass Destruction Directorate, which sponsored the three-day training workshop. “What we do is we identify what our roles are, what our responsibilities are, and how we bring that to the table as a force-multiplier to handle this WMD.”

The workshop is a prime illustration of the WMD Directorate’s mission, which is to prevent a weapon of mass destruction—chemical, biological, radiological, nuclear, or explosive—while at the same time preparing to respond to one. The preventive pieces, or countermeasures, include creating and nurturing relationships with experts in the field—scientists, law enforcement partners, the private sector—so they know how to recognize suspicious activity and how to report it.

“Together, we form strategic partnerships,” said Perren, who attended the training. “We identify the gaps. We identify the vulnerabilities. Together, we develop a plan to address that vulnerability or that gap.”

New Orleans provided a challenging backdrop—it has one of the country’s busiest ports and other critical



**FBI agents and first responders from partner agencies showed some of their equipment at a workshop in New Orleans in May that tested how well they would respond to a disaster involving weapons of mass destruction.**

infrastructures like chemical and power plants that would set off a disruptive ripple effect if attacked. Workshop participants, including attendees from the Department of Homeland Security, the U.S. Coast Guard, and the Department of Defense, along with scores of state and local agencies, said the mock scenario helped them refine their preparedness plans.

**“It opens everyone’s eyes to what the threats and hazards are,”** said Lt. Eric Acosta, a fire safety officer at a port outside New Orleans. “And everyone knows everyone so it’s not like, ‘Who’s he?’ when something happens.”

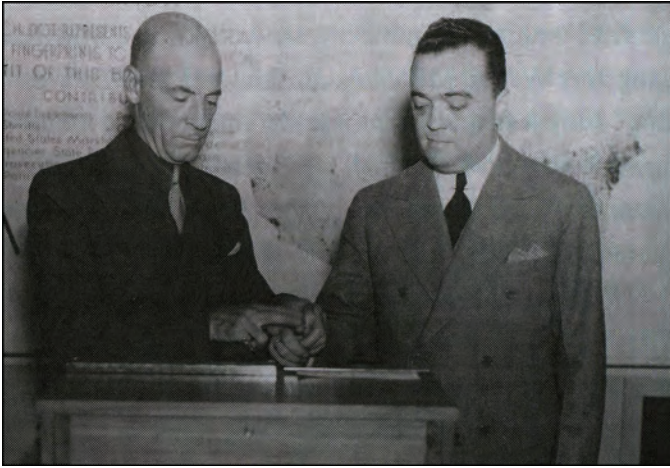
That was a key take-away from the training—having strong working relationships in place makes for a smoother response to any emergency, whether it’s with first-responders or company CEOs. It’s why the FBI has designated WMD coordinators in its 56 field offices—to knit a fabric of connections in their respective regions.

“You play how you practice,” said Stephanie Viegas, a special agent and WMD coordinator in our Miami Field Office, who attended the workshop. “The time to get to know each other is not when something’s happening. It’s having meetings together, going over each other’s operational plans, getting together, and training together so we have the opportunity to recognize and address any gaps.”

In the mock terror scenario, each escalating event prompted a round of questions over who was supposed to do what. Could it have been prevented?

**“What keeps me up at night is not what I know—it’s what I don’t know,”** said Perren. “And that’s why we do these things: to establish tripwires to find out what we don’t know.”





Left: Courtney Ryley Cooper rolls J. Edgar Hoover's fingerprints, circa 1936. *National Archives photo*

## The Hoover Legacy, 40 Years After

### Part 3: Another Side of J. Edgar

The mid-1930s were an important turning point for J. Edgar Hoover's Bureau. It had just defeated a series of dangerous gangsters. Its agents were now heralded as "G-Men." And it was no longer one of several indistinct "Divisions of Investigation." In July 1935, it was given a new name to go with its rising success—the Federal Bureau of Investigation.

Still, the young FBI faced plenty of criticism, some justified and some not. During this time, it worked closely with the Department of Justice (Attorney General Homer Cummings was leading a "war on crime" publicity campaign with respected reporter Henry Suydam) and the news media to tell its story accurately and favorably.

**In 1933, Hoover began working with Courtney Ryley Cooper.** In the early 1930s, Cooper—a veteran author, reporter, and publicist—began writing about the problem of crime in the U.S. and the FBI's growing role in addressing it, including a series of articles for *American Magazine*. His FBI-centered books included *Ten Thousand Public Enemies* (on the criminal underworld), *Here's to Crime* (various criminal activities), and *Designs in Scarlet* (prostitution).

Hoover admired Cooper. The two shared an interest in denouncing the scourge of crime and a vision that the FBI was performing an important public service. As a result, Ryley Cooper (as he was known) came to be a good friend of J. Edgar and a key influence in shaping the Bureau's public image during an often trying time.

Evidence of this relationship is seen in a February 1938 letter that Hoover sent to Cooper's wife, Genevieve, or Gen as Hoover called her. Ryley had just left D.C. after giving a talk at a joint session of the FBI National Academy and the current new agent training class. Hoover told Gen he found Ryley "feeling bad" and thought his viewpoint was "colored through dark glasses." The Director says he tried unsuccessfully to cheer Ryley up.

In what remains of Hoover's writings, the letter is unique. It shows a friendly and personal side of Hoover, who was genuinely concerned about an apparent streak of depression in his friend. The Director himself admits to being "terribly weary and terribly tired," with "tremendous and almost overwhelming worries pressing in on me," but still committed to carrying forward. He signed the letter "Jayee," a nickname used by very few people in Hoover's life, again suggesting his close ties to the Coopers.

It's not clear what happened over the next several years. In 1940, Ryley Cooper began traveling in Mexico and California, digging up information for a story or series on Nazi propaganda and espionage in the United States.

Tragically, after returning to New York in September 1940, Ryley Cooper committed suicide in a hotel room. Initial press reports indicated that Mrs. Cooper thought Ryley might have been depressed on account of an FBI snub. There is no evidence of this, and Hoover thought it unlikely, noting that he hadn't met with Cooper after he returned from his travels nor had he discussed his recent Nazi research with him. Although the 1938 letter hints Ryley's issues with depression were longstanding, the mystery remains as to why he took his own life and what Hoover made of the loss of his friend.

The story of Cooper and Hoover is not well known, but it does shed important light on both Hoover's personality and the FBI's evolving image during a pivotal time in FBI history.

*Part 4: The evolution of U.S. intelligence (page 68)*

## Inside the Denver JTTF

### Part 3: WMD Coordinator Focuses on Preparedness, Partnerships

A chlorine truck explodes on a major highway and a potentially deadly spill occurs. Was it an accident or an intentional act? Livestock become ill from an unidentified organism. Is it a public health issue or an act of domestic terrorism? An official receives a white powder letter. Is it a hoax or a serious threat?

Providing answers to such questions is the job of our weapons of mass destruction (WMD) coordinators, special agents located in each of the FBI's 56 field offices who work with local, state, and federal law enforcement; government; academia; and private industry to counter the WMD threat.

The FBI created the Weapons of Mass Destruction Directorate in 2006 to ensure a coordinated approach to incidents involving nuclear, radiological, biological, or chemical weapons. Carrying out that mission on the ground are the WMD coordinators, whose goal is prevention through preparedness and partnerships.

"When there are potential WMD incidents like a tanker spill or industrial accident, we are very good at assessing them," said Special Agent Dave Autrey, the WMD coordinator in our Denver office. "Usually, we can quickly discern if there is any link to terrorism."

Working through the Joint Terrorism Task Force (JTTF), Autrey relies on a network of organizations in Colorado—from first responders to executives at the state's Department of Public Health. "I reach out on a regular basis to nearly 80 different agencies and departments in my area," he said.

That outreach consists of training—everything from threat briefings to tabletop exercises that play out WMD scenarios—to building relationships. "You don't want to meet a partner from another agency for the first time on the scene of an incident," Autrey said. "That puts everybody behind the curve."

"The idea is to get people on the same page," he added. "If everyone is properly prepared and sharing information during an emergency response, firefighters and other first responders can know exactly what they are dealing with before they even get to the scene. And law enforcement can rapidly determine if the incident is terrorist-related."



FBI agents train with local responders during a WMD exercise in May.

A key resource for Autrey is the Colorado Information Analysis Center (CIAC)—a multi-agency fusion center designed to use intelligence to facilitate criminal and other investigations.

Robin Koons, a Ph.D. epidemiologist with the Colorado Department of Public Safety, works full-time at the fusion center as an analytical supervisor. She is a subject matter expert in biological, chemical, and radiological agents. Koons works closely with Autrey on WMD matters and praises the Bureau's intelligence-driven, all-inclusive approach.

"We have a very solid relationship with the FBI," she said. "The strength of that relationship can especially be seen during suspicious powder events. Working together, we are able to quickly exchange information on the scene between the fire department, health department, and other responders, and then the JTTF coordinates the information coming in to form a complete picture of the threat."

The exchange of information "absolutely works," Koons added. "And a big part of why it works is because Dave puts in a lot of time building relationships."

"The FBI relies heavily on our state partners," Autrey explained. "They are the experts in their regions, and they know all the players. To effectively deal with the WMD threats we face requires everyone to work together."



Left: Agents at firearms training in the 1980s.

## Celebrating Women Special Agents

### Part 3: Early Pioneers Tell Their Stories

*"It was a wonderful experience. I wouldn't trade any of it for the world. And you know, I hope in some small way, maybe I made it easier for women after me."*

That sentiment—shared by former Special Agent Linda Dunn, who served from 1973 to 1976—was echoed by many of the trailblazing women who signed up to be the first female agents in the modern era.

**Their compelling and often moving stories can be found in a series of interviews of retired Bureau investigators—both women and men—conducted by the Society of Former Special Agents of the FBI and posted on the website of the National Law Enforcement Museum.**

It was in 1972—40 years ago this year—that women were allowed to join the ranks of FBI agents, reversing a policy that had been in place since the 1920s. Their reminiscences several decades later reflect the diversity of their motivations, experiences, and achievements. Yet, as you read their stories, you can see that these early female pioneers wanted the same things—to serve their country, to make a difference, to be successful at what they did... just like the men.

**They faced their share of challenges, to be sure.** The physical requirements of the new agent training, originally developed for men, were difficult. Some women struggled with pushups or running; for others, it was boxing and wrestling. Some said they even faced resentment for taking a man's place at the Academy.

Once on the job, some women agents encountered bosses who weren't supportive or an occasional chauvinistic man. Many were thrust into the most dangerous undercover work, since criminals didn't suspect that females would be agents. For these early women, the standards of success were often higher than that of the men. As former Special Agent Nancy Fisher (1978-2004) pointed out, "You had to be very good. ... My friends and I, the female agents, would always say, 'Why is it we have to work so hard to just to be considered average?'"

**For the most part, though, these early female agents were given plenty of support and opportunities to succeed.** During the Quantico training, most men were accepting and helpful, going out of their way to run or workout with the women, for example. Former Agent Yvonne Graham (1978-2001) said, "The guys couldn't have been more supportive, more generous of their time..."

Once in their field offices, the women soon proved any doubters wrong with their work. They found the support of their supervisors and colleagues incredibly helpful. Former Special Agent Natalie Gore (1976-1986) said, "My first office was Seattle, and that SAC (Special Agent in Charge) there was very much in favor of me being there. And that made a huge difference in how the entire office dealt with women in the field."

These women agents went on to work some landmark cases—the Patty Hearst kidnapping, the Reagan assassination, the Unabomber murders, and the attacks of 9/11, to name just a few. Over time, they made lasting contributions, not only by paving the way for their colleagues but by becoming leaders at every level of the organization.

Former Special Agent Birdie Pasenelli—the first woman special agent in charge and assistant director—summed it up by saying, "All I ever asked for is, give me an equal shot at doing this, and I'll prove myself."

She certainly did, just like all these pioneering women agents.

*Part 4: Pop culture's take on women special agents (page 71)*



## A Sordid Scam

### Two Receive Life Sentences for Preying on Aspiring Models

Some of the aspiring young models thought they were getting the chance of a lifetime when they showed up in South Florida to audition for a man they believed to be a legitimate talent scout. Instead, they were drugged and raped on camera—and the resulting videos were sold on the Internet.

The two men responsible for this depraved scheme—one a former police officer and the other a self-described porn star—were each sentenced to 12 consecutive life terms in prison earlier this year, thanks in part to the investigative efforts of Special Agent Alexis Carpinteri, Det. Nikki Fletcher of the Miramar Police Department, and the U.S. Attorney's Office for the Southern District of Florida.

**“These are probably two of the worst offenders I have ever seen,” said Carpinteri, who works in our Miami office. “There were many more victims than the multiple women who were represented at trial.”**

Beginning in 2006, if not before, the subjects used Internet modeling sites as their “hunting grounds” to lure potential victims, Carpinteri said. They understood the industry well enough to impersonate representatives from major multinational companies.

The young women, many aged 18 to 22, agreed to come to Miami believing they were auditioning for a commercial for a prominent liquor company. They were persuaded to come alone because they were told family or boy-friends would be a distraction. The former police officer, Lavont Flanders, Jr., “was not stupid,” Det. Fletcher said. “He knew how to manipulate people, and he could be charming.”

The women were told they would be doing a test shoot in which they would have to drink the liquor they would be advertising. But the alcohol was laced with a date-rape drug that made them extremely compliant and often left them with no memories of what had happened to them. After the drugs took effect, the women were encouraged to sign model release forms.

Based on those consent forms, Carpinteri said, “The subjects thought they were going to get away with it.” Initially, investigators and prosecutors were “disturbed by the videos” because it appeared the victims were willing participants. But the raw footage told a different story.



A digital camera is documented as evidence in the case.

“It was clear the women were drugged and often barely conscious,” Carpinteri said.

**“Because of their memory loss, a lot of the victims swore that nothing had happened,” she added, “until we showed them the videos.”** Other women woke up in their cars the next morning bleeding, covered in vomit, and disoriented. Some notified police.

In 2007, Flanders and his partner, Emerson Callum, were arrested and charged by the state of Florida with multiple counts, including sexual assault and distribution of a controlled substance. Released on bond pending trial, the pair eventually began victimizing women again.

That’s when Carpinteri and Fletcher began working on the case to painstakingly unravel the scam. They identified and interviewed victims from various locations and pieced together evidence from police reports, rape treatment center examinations, DNA results, and cell phone records to help build a case for federal prosecutors. The subjects were indicted federally in 2011 and later convicted by a jury of sexual battery, human trafficking, and other charges.

“This was a difficult case,” Fletcher said, “but it had a good outcome. It’s very satisfying to know that these two individuals will never do this to anyone again.”



Scan this QR code with your smartphone to watch a related video, or visit <http://www.fbi.gov/news/videos/>.



Left: Example of monitor display when a computer is infected with Reveton ransomware.

## New Internet Scam 'Ransomware' Locks Computers, Demands Payment

There is a new “drive-by” virus on the Internet, and it often carries a fake message—and fine—purportedly from the FBI.

**“We’re getting inundated with complaints,” said Donna Gregory of the Internet Crime Complaint Center (IC3), referring to the virus known as Reveton ransomware, which is designed to extort money from its victims.**

Reveton is described as drive-by malware because unlike many viruses—which activate when users open a file or attachment—this one can install itself when users simply click on a compromised website. Once infected, the victim’s computer immediately locks, and the monitor displays a screen stating there has been a violation of federal law.

The bogus message goes on to say that the user’s Internet address was identified by the FBI or the Department of Justice’s Computer Crime and Intellectual Property Section as having been associated with child pornography sites or other illegal online activity. To unlock their machines, users are required to pay a fine using a prepaid money card service.

“Some people have actually paid the so-called fine,” said the IC3’s Gregory, who oversees a team of cyber crime subject matter experts. (The IC3 was established in 2000 as a partnership between the FBI and the National White Collar Crime Center. It gives victims an easy way to report cyber crimes and provides law enforcement and regulatory agencies with a central referral system for complaints.)

“While browsing the Internet, a window popped up with no way to close it,” one Reveton victim recently wrote to the IC3. “The window was labeled ‘FBI’ and said I was in violation of one of the following: illegal use of downloaded media, under-age porn viewing, or computer-use negligence. It listed fines and penalties for each and directed me to pay \$200 via a MoneyPak order. Instructions were given on how to load the card and make the payment. The page said if the demands were not met, criminal charges would be filed and my computer would remain locked on that screen.”

The Reveton virus, used by hackers in conjunction with Citadel malware—a software delivery platform that can disseminate various kinds of computer viruses—first came to the attention of the FBI in 2011. The IC3 issued a warning on its website in May 2012. Since that time, the virus has become more widespread in the United States and internationally. Some variants of Reveton can even turn on computer webcams and display the victim’s picture on the frozen screen.

“We are getting dozens of complaints every day,” Gregory said, noting that there is no easy fix if your computer becomes infected. “Unlike other viruses,” she explained, “Reveton freezes your computer and stops it in its tracks. And the average user will not be able to easily remove the malware.”

The IC3 suggests the following if you become a victim of the Reveton virus:

- Do not pay any money or provide any personal information.
- Contact a computer professional to remove Reveton and Citadel from your computer.
- Be aware that even if you are able to unfreeze your computer on your own, the malware may still operate in the background. Certain types of malware have been known to capture personal information such as user names, passwords, and credit card numbers through embedded keystroke logging programs.
- File a complaint and look for updates about the Reveton virus on the IC3 website at [www.ic3.gov](http://www.ic3.gov).

# Insider Trading

## Proactive Enforcement Paying Off

Last week, an executive with a global pharmaceuticals giant headquartered in the U.S. was arrested for insider trading. He allegedly earned “substantial profits” by trading stock options using inside information about three companies his firm was looking to acquire before they were sold.

**Insider trading is just that:** the trading of securities or stocks by “insiders” with material, non-public information pertaining to significant, often market-moving developments to benefit themselves or others financially. These developments can include pending mergers and acquisitions, anticipated earnings releases, and product line developments.

The universe of people with access to this non-public information is growing. It includes:

- Securities professionals (traders and brokers);
- Corporate executives and employees, along with employees of banking and brokerage firms and even contractors;
- Lawyers working with companies on mergers and acquisitions;
- Government employees who misuse their legitimate need-to-know position; and
- Even friends, family members, and business associates who are tipped off about the information.

In addition to this insider knowledge, all of these individuals have another thing in common: the obligation to keep this information in the strictest confidence.

**Historically, insider trading cases were usually handled as isolated incidents where trading was based on a specific instance of material, non-public information being provided.**

And these cases have been challenging: investigators have relied on financial documents, phone records, and—more recently—e-mails to determine when and how traders receive the non-public details. These criminal insiders work hard to thwart law enforcement—including trading through multiple accounts, trading in others’ names, and using disposable cell phones and prepaid calling cards.

**But we’ve become much more proactive these days...**



using intelligence as well as sophisticated techniques like undercover operations to identify the most egregious offenders. We’ve been able to link seemingly unrelated cases and uncover large criminal rings of insider trading. And our new national Fair Markets Initiative will further focus our insider trading efforts by prioritizing cases, enhancing collaboration with the Securities and Exchange Commission (SEC), and increasing our emphasis on intelligence to identify and dismantle insider trading schemes.

Our growing caseload reflects the wisdom of our approach—we’ve had a 40 percent increase in insider trading cases over the past year.

**Coordination with our partners is vital to this success.** We work very closely with the SEC in a parallel law enforcement and regulatory effort to ensure fairly operated financial markets. In fact, we recently embedded an FBI agent with the SEC in New York.

The FBI also maintains a relationship with the North American Securities Administrators Association—composed of state and provincial securities regulators in the U.S. and Canada—making presentations, offering training, exchanging best practices, etc.

Increasing globalization has led some of our insider trading investigations overseas, where our legal attachés use existing relationships with their partners to follow up on leads. Individuals engaged in illicit insider trading often funnel money through offshore accounts, and overseas employees of American companies with operations abroad could be just as susceptible to the lure of insider trading.

Insider trading has been a continuous threat to U.S. financial markets and has robbed the investing public of some degree of trust that markets operate fairly. Through our investigations, the FBI is working hard to curb that corruption and help ensure fairness in the marketplace.





**Left: Director Hoover receives the National Security Medal from President Dwight Eisenhower on May 27, 1955, as then-Vice President Richard Nixon and others look on.**

## The Hoover Legacy, 40 Years After

### Part 4: The Evolution of U.S. Intelligence

Standing outside the White House on a sunny day in May 1955, President Dwight Eisenhower smiled as he pinned the National Security Medal on the lapel of one of its first recipients—FBI Director J. Edgar Hoover.

In the citation, the president recognized Hoover's "outstanding contribution to the national security of the United States" through "his exceptional tact, perceptiveness, judgment, and brilliant leadership in a position of great responsibility."

**The medal had been created only two years earlier by President Truman to recognize individuals—civilian and military—who had made important contributions to national security in the field of intelligence.** The honor has since been supplanted by the National Intelligence Distinguished Service Medal.

Given that many Americans associate the early Bureau with chasing gangsters and solving murders and other violent crimes, it might seem unusual for a law enforcement leader to have been given such an award at that point in history. But Hoover, as it turns out, had played a key role in the evolution of the U.S. intelligence community and the transformation of the FBI into a national security organization.

**That evolution took place over several decades.** Hoover joined the Department of Justice two months after the U.S. entered World War I, when intelligence issues were a top priority. Within two years, he was appointed to head

a new General Intelligence Division—also called the Radical Division—in response to widespread domestic terrorist attacks. The purpose of the division was to gather intelligence about terrorist threats and determine whether or not they were connected to foreign revolutionary movements.

Hoover continued his rise in the department and by 1924 was leading the Bureau of Investigation, the FBI's predecessor. But during the 1920s, the U.S. faced few major national security threats. And excesses in the Bureau's response to anarchist violence led to a tempering of domestic intelligence work during the decade.

**In the mid-1930s, though, the security picture was changing.** Evidence of Japanese and German (and to a lesser extent, Soviet) espionage began to accumulate, and the FBI was called upon to investigate. With the start of World War II, these responsibilities expanded dramatically, with Hoover's FBI being tapped to handle domestic counterintelligence and the collection of foreign intelligence in the Western Hemisphere.

Throughout this time, Hoover dealt with a number of challenges. There was no U.S. intelligence community of any real size or complexity before the war, so the FBI became a key part of a rapidly growing group and Hoover a founding father. The number of players in the intelligence realm was large, and inevitable disagreements arose in the midst of some remarkable cooperation. Hoover played a central role in sorting out jurisdictional issues, addressing the inefficiencies of overlapping responsibilities, and helping the FBI and its partners navigate the steep learning curve of intelligence.

As the war ended and Soviet espionage became clear, Hoover's FBI took its hard-won knowledge of intelligence and its tradecraft and shifted its attention to the new threat, uncovering earlier Soviet efforts and moving proactively against its current and future operations.

The end result of Hoover's leadership was not just the National Security Medal, but a stronger and more capable Bureau that would play a key role in America's national security structure for decades to come.

*Part 5: A day in the life (page 79)*

## Mortgage Fraud

### ‘House King’ was a Royal Con Man

When most people buy a home they are required to submit financial paperwork to banks, title companies, and others involved in the mortgage process. The case of the “House King” in South Florida illustrates how when fraudsters manipulate that system, lenders can lose millions—and innocent buyers and sellers also suffer.

“Imagine,” said Special Agent Denise Stemen, “a world where buyers don’t fill out any mortgage paperwork—and don’t even read it—because everything on the application is a lie.”

The House King, Angel Puentes, used a classic loan origination scam, said Stemen, a veteran mortgage fraud investigator in our Miami office. “In this scheme, you had all the players,” she explained, from straw buyers—who were paid to lend their name to documents—to a real estate agent, licensed mortgage broker, and title attorney. Mortgage applications were falsified to inflate the value of properties, defraud lenders, and line the pockets of the fraudsters.

Puentes—also known as D’Angelo Salvatore—was so influential he created his own glossy real estate magazine called *House King*. “Five or six years ago, he was the guru of South Florida real estate,” said Special Agent Mark Soucy, who investigated the case, adding that “100 percent of the funding for the magazine came from the fraud he was committing.”

**The House King paid straw buyers to sign bogus mortgage applications claiming that purchased homes would be their primary residences—when in reality, they had no intention of living there.** The fraud was so extensive that some buyers had closings with three different lenders on the same day.

An attorney signed off on the fake documents, and the lenders—believing everything was legitimate—made the loans. The applications also inflated the value of the properties. If a home was appraised at \$400,000, for example, the bogus loan application might list the value at \$500,000. Puentes pocketed the extra money and used it to pay his accomplices. He then paid the mortgage for a number of months until he could flip the property for a further profit—or sometimes he rented it out to generate more income. But then he stopped paying. After taking his ill-gotten profit, Puentes simply walked away



Angel Puentes—also known as D’Angelo Salvatore—was so influential he created his own glossy real estate magazine called *House King*. The publication’s masthead is seen above.

from the mortgage, leaving the lender with a toxic asset. Meanwhile, he was living large, taking trips to Paris and buying a Ferrari.

We began investigating Puentes in 2008. At the time, before the real estate market began to collapse in South Florida and around the country, many speculators were buying properties and trying to flip them for quick profits. But Stemen said, “Our investigation focused on the organized group that was falsifying documents to profit from the loan origination schemes.”

**Puentes was indicted in February 2011 on multiple counts of wire and bank fraud and for defrauding three lending institutions out of approximately \$10.5 million.** Although he fled the country for a time, Puentes eventually returned and was arrested. In June 2011, he was sentenced to more than eight years in prison.

Because of fraudsters such as Puentes, South Florida real estate was artificially inflated and innocent people paid too much for their homes. When the market crashed, many of those homeowners were left underwater—their property worth less than what they paid for it.

“Those are the true victims of this type of mortgage fraud,” Soucy said—“the legitimate South Florida residents whose home values were inflated because of these fraudulent transactions.”



Left: A burial site on the outskirts of Kigali, Rwanda for some of the victims of the 1994 genocide. Photo courtesy of The U.S. Holocaust Memorial Museum

## Genocide and War Crimes

### New Webpage Designed to Raise Awareness, Solicit Information

Kosovo...Rwanda...Srebrenica. These places will forever be associated with unspeakable, brutal acts of genocide and war crimes.

The global community has banded together to help prevent crimes like these and to bring to justice the perpetrators who commit them. The U.S. is part of this international effort—most recently through the creation of an interagency Atrocities Prevention Board. And the FBI supports the government's efforts through its own Genocide War Crimes Program.

Today, in an effort to raise awareness about these crimes and the FBI's part in helping to combat them, we're announcing the launch of our Genocide War Crimes Program webpage. In addition to educating the public on our role, the website solicits information from victims and others about acts of genocide, war crimes, or related mass atrocities that can be submitted to us through [tips.fbi.gov](http://tips.fbi.gov) or by contacting an FBI field office or legal attaché office.

**Why is the FBI involved, especially since these incidents primarily take place overseas?** Take a look at the jurisdiction section of our new website, which explains the 1998 Presidential Executive Order 13107 and the four U.S. laws dealing with genocide, war crimes, torture, and recruitment or use of child soldiers.

According to Special Agent Jeffrey VanNest, who heads up our Genocide War Crimes Unit (GWCU), our mission is to "systematically and methodically help track down

perpetrators of genocide, war crimes, and other related atrocities—the worst of the worst—and apprehend them."

**These types of investigations are among the most complex ones we work.** They typically involve piecing together fragmentary bits of information, interviewing overseas witnesses in conflict zones, collecting evidence in other countries, and accommodating language barriers. And the key to successfully conducting them—according to VanNest—is cooperation.

"The GWCU works shoulder-to-shoulder with our U.S. federal partners—most often with the Department of Homeland Security's Immigration and Customs Enforcement (ICE)—to determine if there's a violation of U.S. law," says VanNest. "If so, we envision working many of these cases jointly with our partners in ICE's Homeland Security Investigations."

Internationally—because the bulk of these investigations occur overseas—we work through our network of legal attachés who have established relationships with our counterparts in foreign nations and who coordinate our work with international criminal tribunals. We also cooperate with INTERPOL.

On the overview section of our new webpage, you can find out more about how we offer additional support—such as crime scene preservation, interviewing techniques, age-enhancing photos, language services, and increasingly, victim/witness services—to foreign authorities and who our primary domestic and international partners are.

Members of the GWCU, usually in conjunction with our ICE counterparts, coordinate our genocide/war crimes investigations. Collectively, GWCU agents and intelligence analysts in the unit are carefully selected for what they can bring to the table—subject matter expertise, interviewing skills, experience in past critical incident response, foreign language ability, and experience working with partner agencies in the U.S. and abroad.

**"Our ultimate goal," says VanNest, "is to ensure that perpetrators of these heinous crimes find no safe haven in the United States, or for that matter, no safe haven anywhere in the world."**



# Celebrating Women Special Agents

## Part 4: Who Said It? Pop Culture's Take on Women Special Agents

1. "I am in a dress, I have gel in my hair, I haven't slept all night, I'm starved, and I'm armed! Don't mess with me!"
2. "You see a lot, doctor. But are you strong enough to point that high-powered perception at yourself? What about it? Why don't you—why don't you look at yourself and write down what you see? Or maybe you're afraid to."
3. "He was kinda of cute...for a sociopath."
4. "Hey, you think it's easy being surrounded by guys with guns all day?"  
*Male agent: "I thought you liked guys with guns."*  
*"I like the guns."*
5. "What are you doing here?"  
*Male scientist: "We're trying to plug a hole in the universe. What are you doing here?"*  
*"Apparently the same thing."*
6. "Sometimes looking for extreme possibilities makes you blind to the probable explanation right in front of you."
7. "Journalist William D. Tammus wrote: You don't really understand human nature unless you know why a child on a merry-go-round will wave at his parents every time around and why his parents will always wave back."
8. "A cup of tea, a German-English dictionary, and I'll have it translated in a day or two."

It took a while for Hollywood and television to notice that FBI women special agents had come on the scene in 1972—and to think how they might work into old and new storylines. At first, in the early 1990s, the focus was on training and new agents...and on comedy—women trying by hook or by crook to make it in a man's profession. Now you find our women agents portrayed in a variety of decisive roles in team environments—trying to locate missing persons, analyzing evidence, analyzing the criminal mind, and, of course, investigating paranormal activity and worldwide conspiracies. We think it's just



**A scene from *The X-Files*, which featured agents investigating paranormal phenomenon. Hint: the female agent pictured here said one of the quotes in the quiz.**

a matter of time before women agents are cast as the operational leaders they are in real life.

### Key to the Quiz

1. Special Agent Gracie Hart (Sandra Bullock) is an FBI agent in *Miss Congeniality* (2000) who isn't entirely happy about going undercover in the Miss United States beauty pageant to prevent a group from bombing the event.
2. Special Agent Clarice Starling (Jodie Foster), fresh out of new agent training, verbally spars with the perfidious Hannibal Lecter in the 1991 film *Silence of the Lambs*.
3. New Agent Janis Zuckerman (Mary Gross) teams with Ellie DeWitt (Rebecca De Mornay) in *FEDS* (1988) to try to get through the hazing and hazards of FBI new agent training.
4. Special Agent Samantha "Sam" Spade (Poppy Montgomery) works on a fictional Missing Persons Squad in New York City in the television series *Without a Trace*, which ran from 2002 to 2009.
5. In a series with parallel universes, Special Agent Olivia Dunham (Anna Torv) is part of a multi-agency task force investigating strange crimes with the help of an institutionalized scientist in *Fringe: There's More Than One of Everything* (2009).
6. Special Agent Dana Scully (Gillian Anderson) waxes philosophical with her partner Fox Mulder (David Duchovny) in the television science fiction drama *The X-Files*, which ran from 1993 to 2002.
7. In *Criminal Minds: Cradle to Grave* (2009), Special Agent Jennifer "JJ" Jareau gives her signature voiceover to an episode featuring the fictional casework of the FBI's Behavioral Analysis Unit at the FBI Academy in Quantico, Virginia.
8. Special Agent Diana Barrigan (Marsha Thomason) sets Peter Burke straight in the "Deadline" episode of *White Collar* (2009).

*Part 5: A diversity of backgrounds and experiences (page 72)*



**Left: Brenda Heck, on competing to be on the FBI Hostage Rescue Team in 1993:** “I was driven by the challenge. It didn’t even occur to me that I was being questioned because I was a female. It just never occurred to me. I imagine I probably surprised a few people.”

## Celebrating Women Special Agents

### Part 5: A Diversity of Backgrounds and Experiences

In the 40 years since the FBI began training women to be special agents, many have said it was a dream they had held since childhood. They played cops and robbers as kids, kept their noses clean, and maybe joined the military or the local police, consciously burnishing their credentials on the road to becoming G-Women.

“I’m not quite sure where the seed got planted,” said Katrina G., an agent who now runs the Bureau’s Forensic Audio Video and Image Analysis Unit. “But I thought the FBI—fidelity, bravery, integrity—you can’t go wrong. I always wanted to be someone to do the right thing, to be fair and honest, and to stick up for the little guys.”

Others followed a less scripted route. Shelia T., an agent at the FBI’s Regional Computer Forensic Laboratory in Quantico, Virginia, set out in college to be a research professor and was well on her way when she drove a friend to an FBI recruitment event on campus. “We went in and sat through the session,” she recalled. “My friend is listening because she’s interested, and I’m in the back waiting for her to finish so we can go study.” An agent suggested Shelia apply, too. She found herself at the FBI Academy for new-agent training on August 16, 1998. A few years later, she was in Ken Lay’s office at Enron, collecting evidence at the center of the Bureau’s largest-ever white-collar crime scene.

Their stories, revealed in more than a dozen interviews with female agents past and present, show there’s no well-defined template for women agents, apart from a desire to serve. Like the first two women agents—a nun and a Marine—they arrived at the FBI with varied backgrounds and proceeded to have similarly varied careers. In video interviews, they talk about what brought them to the Bureau, the challenges they faced, their unique work experiences, and their reflections on careers that broke more than a few glass ceilings.

A common thread is that none aspired to be great women agents, just great agents that happened to be women.

Here’s a preview:

- **A 24-year agent who early in her career competed for a spot on the all-male Hostage Rescue Team:** “I was driven by the challenge. It didn’t even occur to me that I was a female and that I was being questioned because I was a female.”
- **A retired agent who rose through a series of leadership firsts to the Bureau’s third-highest position:** “At the time, when women became the first at anything, somebody always took notice. And often it was the women who took notice because we were trying to find our way and make sure that we had the opportunities that men who were agents had. And we did.”
- **Special agent in charge of the Anchorage Division:** “I think women coming through today, they benefit from the experiences of all the women that have gone before and the fact that it’s not considered so unusual now.”

The growing ranks of women agents echo the Anchorage agent’s comments—there are more than 2,600 today, including 11 in charge of field offices. “As a whole, the Bureau is better for having women agents,” she said. “I think we make the Bureau more complete.”

*Part 6: Working undercover (page 78)*



Scan this QR code with your smartphone to watch one in a series of related videos, or visit <http://www.fbi.gov/news/videos/>.

# A Byte Out of History

## Murder and the Dixie Mafia

This month marks the 25th anniversary of the murder of Judge Vincent Sherry and his wife, Margaret, whose deaths at the hands of the so-called Dixie Mafia exposed the lawlessness and corruption that had overtaken Mississippi's Gulf Coast in the 1980s.

**“It was out of control,”** said retired Special Agent Keith Bell, referring to the level of corruption in Biloxi and Harrison County—so much so that in 1983 federal authorities would designate the entire Harrison County Sheriff’s Office as a criminal enterprise. Special Agent Royce Hignight initiated the investigation of the sheriff and was soon joined by Bell.

**“They were doing anything and everything illegal down here,”** said Bell, who grew up on the Gulf Coast. **“For money, the sheriff and officers loyal to him would release prisoners from the county jail, safeguard drug shipments, and hide fugitives. Anything you can think of, they were involved in.”**

Bell is quick to point out that there were plenty of honest officers on the force, and some would later help the FBI put an end to the culture of corruption in Biloxi. But for a long time, Sheriff Leroy Hobbs and his Dixie Mafia associates held sway.

The Dixie Mafia had no ties to La Cosa Nostra. They were a loose confederation of thugs and crooks who conducted their criminal activity in the Southeastern United States. When word got out that Biloxi—with its history of strip clubs and illicit gambling—was a safe haven, the criminals settled in.

At the same time, members of the organization incarcerated at the Louisiana State Penitentiary at Angola were running a “lonely hearts” extortion scam with associates on the street. The scam targeted homosexuals and brought in hundreds of thousands of dollars—money they entrusted to their lawyer, Pete Halat.

But Halat, who would later become mayor of Biloxi, spent the money. When it came time to hand it over to the crooks, he said the cash had been taken by his former law partner, Vincent Sherry. So the Dixie mob ordered a hit on Sherry, a sitting state circuit judge who had no direct ties to the criminals. On September 14, 1987, Sherry and his wife were murdered in their home.



**“Gulf Coast residents were shocked by the murders,”** Bell said. Local authorities worked the case unsuccessfully for two years. The FBI opened an investigation in 1989, and Bell was assisted in the investigation by Capt. Randy Cook of the revamped sheriff’s office—Leroy Hobbs was convicted of racketeering in 1984 and sentenced to 20 years in prison.

The federal investigation into the Sherry murders lasted eight years. In the final trial in 1997, Pete Halat was sentenced to 18 years in prison. Kirksey McCord Nix—the Dixie Mafia kingpin at Angola who ordered the hits—as well as the hit man who killed the Sherrys each received life sentences.

As a result of the cases, Bell said, **“Gulf Coast citizens started demanding more professional law enforcement and better government.”** Bell—who wanted to be an FBI agent since he first watched *The FBI* television series as a child—added, **“It meant a lot to me to return to my home and do something about the corruption that had worked its way into government and law enforcement there.”** He added, **“The majority of citizens realized that if the FBI had not stepped in, the lawlessness and corruption would likely have continued unabated.”**





## Infant Abductions

### A Violent Trend Emerges

It is relatively rare for infants to be abducted by strangers. But it does happen. And recent analysis of abduction cases by the FBI suggests there are new and troubling trends for expectant parents to be aware of, including women kidnappers using violence to commit their crimes and social media to target their victims.

**In April, for example, a 30-year-old Texas woman shot and killed a 28-year-old mother while kidnapping her 3-day-old son from a pediatric center. The infant was recovered six hours later.**

“For the most part, women are no longer going into hospitals and dressing in nurse’s uniforms and walking out with children,” said Ashli-Jade Douglas, an FBI intelligence analyst who works in our Crimes Against Children Unit and specializes in child abduction matters. That’s because hospital security has greatly improved over the years.

A recent case illustrates the point: Last month, a woman entered a California hospital dressed in medical scrubs and abducted a newborn girl, hiding the baby in a bag. But when she attempted to walk out of the hospital, the baby’s security bracelet triggered an alarm and the woman was caught.

Because of heightened hospital security, Douglas said, “now women who desperately want a child—and are willing to go to extreme lengths to get one—have to gain direct contact with their victims, and that’s when things can turn violent.”

“The women who commit these crimes are usually between the ages of 17 and 33,” said Douglas, who provides analytical support to our Child Abduction Rapid Deployment Team. “Usually, they are unable to get

pregnant. Often, they will fake a pregnancy in the hopes of keeping a boyfriend or husband.” In most cases, she added, the women intend no harm to the infants—and maybe not even the mother. “They just want a child to raise as their own and will do anything to get one.”

Another emerging trend, Douglas said, is that women desperate for a child are turning to social networking websites to locate victims. “We have seen several recent cases involving social networking sites,” she explained, “and we see how easy it is to use these websites to gain access to targets.”

In January, for example, a 32-year-old Florida woman developed a friendship with a younger new mother through a social networking site. The woman lied about having her own newborn and claimed the child was sick and in the hospital. The victim invited the woman to spend the night at her house, and the next morning, when the victim was in the shower, the woman abducted her 2-week-old infant. She then deleted her contact information from the victim’s social networking site, thinking she would not be found. The baby was recovered and the woman was arrested.

“Parents should check their privacy settings on social networking sites,” Douglas said, and they should always use caution on the Internet. Without the proper settings, pictures posted online can contain embedded information that allows others to track your movements.

“This information is important to share with parents,” Douglas said. “They should be aware of their physical surroundings and how they use the Internet. This can help protect mothers and their babies.”

## 30-Year-Old Murder Solved

### Fingerprint Technology Played Key Role

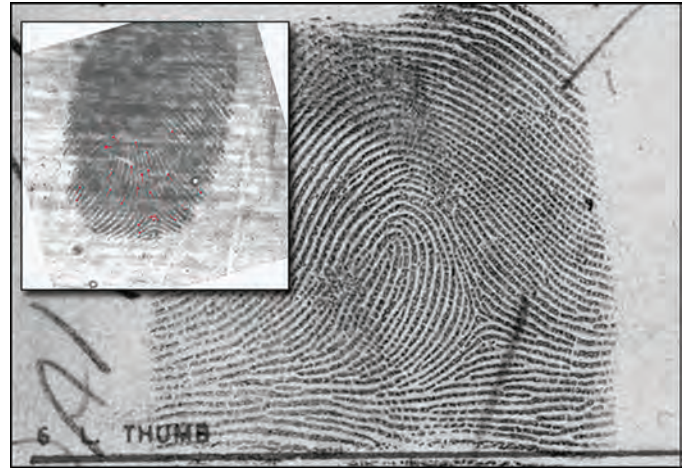
A cold case is just that—an investigation of a crime, usually a violent one, where all leads have been exhausted and the trail has gone cold. But in recent years, the use of various technologies has begun heating up many of these cold cases, uncovering new leads for investigators and providing justice for victims.

One immediate technology example that comes to mind is automated fingerprint searching—more precisely, searches of latent prints of violent unknown perpetrators left at crime scenes. (Latent prints are impressions—usually invisible to the naked eye—produced by the ridged skin on human fingers, palms, or soles of the feet.) The FBI's Integrated Automated Fingerprint Identification System (IAFIS), which houses known records for approximately 73 million criminal subjects, is used daily by local, state, tribal, and international law enforcement for current cases, but increasingly for help in solving cold cases as well. And once a year, the Bureau's Criminal Justice Information Services Division recognizes an outstanding major case solved with help from IAFIS.

The 2012 Latent Hit of the Year Award was presented last month to two employees of the Omaha Police Department—Detective Douglas Herout and Senior Crime Laboratory Technician Laura Casey—for their efforts to identify the man responsible for a brutal murder more than 30 years ago.

**The crime:** In 1978, 61-year-old Carroll Bonnet was stabbed to death in his apartment. Police collected evidence, including latent fingerprints and palmprints from the victim's bathroom (officers believed the killer was trying to wash off blood and other evidence before leaving the apartment). The victim's car was then stolen.

**The investigation:** The car was found in Illinois, but after collecting additional latent prints, investigators couldn't develop any new leads. The crime scene evidence was processed, and latent prints recovered from the scene and the car were searched against local and state fingerprint files. Investigators also sent fingerprint requests to agencies outside Nebraska, but no matches were returned and the case soon went cold.



A latent thumbprint from the crime scene (inset) was matched to this IAFIS record.

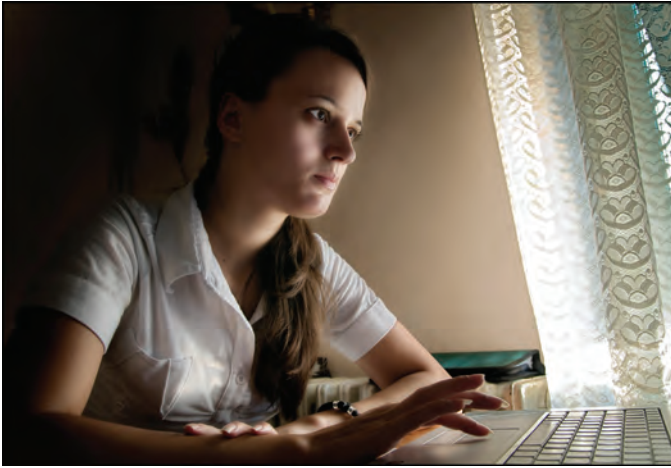
**The re-investigation:** In late 2008, the Omaha Police Department received an inquiry on the case, prompting technician Laura Casey to search the prints against IAFIS (which didn't exist in 1978). In less than five hours, IAFIS returned possible candidates for comparison purposes. Casey spent days carefully examining the prints and came up with a positive identification—Jerry Watson, who was serving time in an Illinois prison on burglary charges.

The case was officially re-opened and assigned to the cold case squad's Doug Herout. Working with laboratory technicians and analysts, Herout reviewed the original evidence from the case, including a classified advertisement flyer with "Jerry W." scribbled on one of the pages. Herout also discovered that Jerry Watson had lived only a few blocks from where the victim's car was recovered.

And the discovery was made just in time—Watson was just days away from being released from prison.

Herout traveled to Illinois to question Watson and presented him with an order to obtain a DNA sample. Subsequent testing determined that Watson's DNA matched DNA recovered at the crime scene, a finding that—combined with Watson's identified prints—resulted in murder charges and a conviction. On October 17, 2011—33 years to the day that Bonnet's body was discovered—his killer was sentenced to life in prison.

It's yet another example of the vital role that technology plays in getting dangerous criminals off our streets.



## Teen Prostitution

### Gang Used Social Media Sites to Identify Potential Victims

It's yet another reason why parents need to keep a close eye on their kids' involvement with social networking websites—during a three-year period ending in March 2012, members of a violent Virginia street gang used some of these websites to recruit vulnerable high-school age girls to work in their prostitution business.

After a multi-agency state and federal investigation, all five defendants pled guilty to various federal charges related to the sex trafficking conspiracy. The leader of the gang—27-year-old Justin Strom—was sentenced on September 14 to 40 years in prison, while the sentences handed down for the other four defendants totaled 53 years.

Strom headed up the Underground Gangster Crips (UGC), a Crips “set” based in Fairfax, Virginia. The Crips originated in Los Angeles in the late 1960s and early 1970s, and since then, the gang has splintered into various groups around the country. Law enforcement has seen a number of Crips sets in the U.S. engaging in sex trafficking as a means of making money.

#### **That's certainly what was happening in Virginia.**

Strom and his UGC associates would troll social networking sites, looking for attractive young girls. After identifying a potential victim, they would contact her online using phony identities...complimenting her on her looks, asking to get to know her better, sometimes offering her the opportunity to make money as a result of her looks.

If the victim expressed interest (and many did, being young and easily flattered by the attention), Strom or one

of his associates would ask for her cell phone number to contact her offline and make plans to meet.

After some more flattery about their attractiveness, sometimes hits of illegal drugs and alcohol, and even mandatory sexual “tryouts” with Strom and other gang members, the girls were lured into engaging in commercial sex, often with the help of more senior girls showing them the ropes. The girls might be sent to an apartment complex with instructions to knock on doors looking for potential customers...or driven to hotels for pre-arranged meetings...or taken to Strom's house, where he allowed paying customers to have sex with them.

In addition to using the Internet, Strom and his associates recruited vulnerable young girls from schools and bus and rail stops. He also went online to find customers—postings ads on various websites showing scantily clad young women.

Some of the juvenile victims were threatened with violence if they didn't perform as directed, and many were given drugs or alcohol to keep them sedated and compliant.

**Strom and his associates did not discriminate—their victims were from across the socioeconomic spectrum and represented different ethnic backgrounds.**

The FBI's Washington Field Office worked the investigation alongside the Fairfax County Police Department, with the assistance of the Northern Virginia Human Trafficking Task Force.

After the group's indictment in March 2012, then-Special Agent in Charge Ronald Hosko of our Washington Field Office reiterated the importance of working with our partners and community groups in combating these types of despicable crimes. He also said, “Trafficking in humans, especially for the purpose of underage prostitution, is among the most insidious of crimes...and the FBI will leave no stone unturned in our efforts to track down those who exploit our children and engage in human trafficking.”



## New Top Ten Art Crime

### Reward Offered for Stolen Renoir Painting

An oil painting by French Impressionist Pierre Auguste Renoir stolen from a Houston home last year—and estimated to be worth \$1 million—is the newest addition to the FBI's Top Ten Art Crimes list.

**The painting, *Madeleine Leaning on Her Elbow with Flowers in Her Hair*, was stolen during an armed robbery on September 8, 2011. The homeowner was watching television when she heard a loud noise downstairs. When she went to investigate, she was confronted by an armed man in a ski mask.**

"We hope that adding the Renoir to the FBI's Top Ten list and publicizing the reward of up to \$50,000 for information leading to the recovery of the painting will prompt someone to come forward," said Peter Schneider, a sergeant with the Houston Police Department who is a member of the FBI's Violent Crimes Task Force in Houston.

Information about the painting has been included in the FBI's National Stolen Art File, as well as other similar online tools—including the Art Loss Register and INTERPOL's Works of Art database—that alert art dealers, gallery owners, and auction houses about missing and stolen artwork.

"If the thief tries to place the painting with a reputable dealer or gallery, or tries to sell it at auction, members of the art community here and overseas who regularly check these databases will see that the artwork has been stolen and will alert the FBI," said Bonnie Magness-Gardiner, who manages the Bureau's art theft program. "Our goal is to provide information about this theft to the widest audience possible," she said.

Renoir, a master Impressionist, painted *Madeleine Leaning on Her Elbow with Flowers in Her Hair* in 1918. The canvas size is 50.17 x 41.28 centimeters, and the artist signed the oil portrait in the lower right corner. The painting was taken with its frame intact from the stairwell where it hung.

**The masked robber, who forced entry through the back door of the home, is described as a white male, 18 to 26 years old, who weighs about 160 pounds and is approximately 5'10" tall. He was armed with a large-caliber, semi-automatic handgun.**



*Madeleine Leaning on Her Elbow with Flowers in Her Hair*

Sgt. Schneider said that while Houston has had its share of art crimes, few have been as high-profile as the theft of the Renoir. He added that the thief would likely try to sell the painting in a larger art community like New York or Los Angeles, or possibly overseas.

The FBI established the Top Ten Art Crimes list in 2005. Since then, six paintings and one sculpture have been recovered, including a Rembrandt self-portrait and another Renoir work titled *Young Parisian* stolen from Sweden's National Museum. The current list may be found on the art theft program page on the FBI Internet website.

**We need your help:** Anyone with information about the stolen Renoir is encouraged to contact their local FBI office or the nearest U.S. Embassy or Consulate, or to submit a tip online at <https://tips.fbi.gov>. A private insurer is offering up to \$50,000 for information leading to the recovery of the painting.



## Celebrating Women Special Agents

### Part 6: Working Undercover

They've played the part of everyone from a college student to a CEO...created and run entire fictitious companies...attended motorcycle gang weddings...even been "arrested" for the good of the cause.

**In the four decades since women have served as FBI agents, they've taken on one of the most difficult—yet vitally important—roles in the Bureau: going undercover.**

Our early female pioneers had a lot of fascinating stories to tell about this work—how dangerous it was, how they gained the trust of criminals, how they used their specialized language and other skills.

Recently, we talked with three current female agents about their undercover experiences. Despite the challenges of the job, all are passionate about their work and believe that women bring unique perspectives that enhance their effectiveness on the job.

Because of obvious sensitivities, we're keeping the identities of these agents confidential.

**Q. What types of cases have you been involved in, and what types of roles have you played?**

Agent #2: "I've worked cases involving outlaw motorcycle gangs, espionage, and public corruption, among others. I've had roles where I was the primary undercover, the secondary undercover, and even had cameo undercover appearances in other undercover operations."

Agent #3: "A variety of cases and roles...for instance, in health care fraud, a patient seeking prescription medicine;

in mortgage fraud, a wealthy investor; in public corruption, a CEO; and in organized crime, a business woman in one case and a girlfriend to a male undercover agent in another."

**Q. What qualities do you think undercover agents need to be successful?**

Agent #1: "I think the FBI needs a variety of people with different qualities for undercover work...a loner would be a great fit for some cases, while a gregarious, outgoing person would be perfect for another."

Agent #3: "Both life and job experiences contribute to being a successful undercover agent—being a team player, having a good work ethic and a sense of humor, staying flexible, and exercising good judgment and common sense. I also think that the many roles we play in real life—wife, mother, girlfriend, etc.—help us get close to our subjects."

**Q. Have the criminals in your investigations ever said anything after they learned who you really were?**

Agent #1: "Yes. Many times, criminals offer us up (as crooked colleagues) when they're trying to cooperate in post-arrest interviews. It's pretty interesting to see how convinced they are that we're really criminals, too!"

Agent #2: "I think the words that sum it up best are, 'No way, I don't believe it!' That makes me feel like I've done my job well."

**Q. What's your most memorable experience while serving undercover?**

Agent #1: "It's difficult to pick one. I've listened to domestic extremists talk about how corrupt the U.S. is; pretended to befriend a dirty drug-dealing cop; been arrested and jailed (twice!); attended high-end poker games; and paid kickbacks to corrupt doctors."

Agent #2: "During a health care fraud case, a target doctor was showing me around his office and offered me free Botox injections in my forehead. I didn't want to make him suspicious, so I got the injections. I had to do a lot of paperwork explaining that one!"

"These women, and others like them," says the agent who currently oversees the Bureau's Undercover and Sensitive Operations Unit, "are a huge asset...many past and ongoing undercover operations owe their successes to the unique perspectives, expertise, and diversity female undercover personnel regularly provide in this elite and demanding area."

*Part 7: Two made the ultimate sacrifice (page 90)*

# The Hoover Legacy, 40 Years After

## Part 5: A Day in the Life

It's 50 years ago today, a warm morning in late September 1962. The 67-year-old J. Edgar Hoover—who by then had served as FBI Director for 38 years—woke up, showered, and dressed.

Hoover's long-time housekeeper, Annie Fields, served breakfast, and the Director shared a fair amount of it with his two Cairn Terriers—Cindy and G-Boy, his third dog by that name.

By 8 a.m., a Bureau driver arrived to get Hoover and then drove a few blocks away and picked up Associate Director Clyde Tolson. Since it was a nice day, the car stopped on Virginia Avenue near the National Mall. The two elderly gentlemen got out and walked the remaining six or seven blocks to the Department of Justice building.

Once inside, Hoover and Tolson took the elevator to the fifth floor. Hoover's office suite was at the corner of the building on Pennsylvania Avenue and 9th Street, and Tolson's was across the hall.

**For the first hour or so, Hoover worked from his private office, reading through the many reports, offering his comments, and issuing his orders on the Bureau's large and diverse number of cases and administrative matters.** His comments—written in blue ink—showed a breadth of knowledge of Bureau activities and, sometimes, revealed Hoover's personality and sharp wit.



Hoover meets with associates in his front office in the 1940s.



J. Edgar Hoover at his desk.

**Just before 10 a.m., Hoover moved to his larger, formal office and began a series of public meetings.** He met with Lieutenant Colonel Jose Lukhan, his counterpart in the Philippines. Then came a visit with Special Agent Robert G. Emond, who was about to become the head of security at the U.S. Information Agency.

Promptly a few minutes before noon, Hoover and Tolson were driven to the Mayflower Hotel for their regular lunch, which lasted an hour. Hoover's afternoon included a meeting with a visiting retired agent and a dental appointment. Shortly after 4:30 p.m., Hoover received a telephone call from President Kennedy's chief of staff, Kenneth O'Donnel; the two talked for some time. Given the developing Cuban Missile Crisis and the impending desegregation of the University of Mississippi, the issue of the call was clearly of national importance.

At 5:20 p.m., Hoover and Tolson left together and were driven to their respective homes. Many days Hoover stayed much later.

**For the aging Hoover, this day—recreated from previously released office logs, FBI files, and other government documents—was a typical one.** The Director would pass away in his sleep just under a decade later, ending his remarkable 48-year run as head of the FBI. His time in office, which represented a period of great cultural and technological change for the nation, was not without its missteps. But as Director, Hoover's intelligence and organizational skills helped turn a small, largely unknown organization into what it is today—a premier national security organization with both law enforcement and intelligence responsibilities, one that protects the nation from a variety of serious threats while providing leadership to its partners around the world.





**Left: National Academy students who successfully tackle the “Yellow Brick Road,” a grueling 6.1 mile run and obstacle course, receive a yellow brick to signify their accomplishment.**

## FBI National Academy

### Celebrating a Milestone

The FBI’s National Academy, known as one of the premier law enforcement training programs in the world, graduated its 250th class earlier this month, and the graduates—like thousands who preceded them—returned to their police departments and agencies in the U.S. and overseas with new knowledge and many new friends.

“I have made some true friends for life,” said Kenneth Armstrong, detective chief inspector of the Strathclyde Police in Glasgow, Scotland, referring to his classmates from the 10-week program held at the FBI’s training facility in Quantico, Virginia.

**Established in 1935, the National Academy provides advanced investigative, management, and fitness training to senior officers who are proven leaders within their organizations.** In addition to undergraduate and graduate-level college courses offered in areas such as law, behavioral and forensic science, understanding terrorism and terrorists, and leadership development, students forge lasting connections that strengthen global law enforcement partnerships.

“If you’re a National Academy graduate,” said Special Agent Greg Cappetta, chief of the National Academy Unit at Quantico, “it doesn’t matter where you go in the world—someone there has gone through the program and will be ready to help you.”

To date, more than 46,000 men and women have graduated from the program, and more than 28,500 are still active in law enforcement work. The 250th graduating class, consisting of 264 officers, came from 49 U.S. states and 24 countries.

“The amount of knowledge is so vast among National Academy students that there is pretty much no law enforcement problem that can’t be solved,” Cappetta tells classes when they first arrive at Quantico. “Whatever problem you might be having in your police department, there is someone in the session who has gone through the same thing.”

Michael Connolly, a captain in the San Francisco Police Department who graduated with this most recent class, agreed. “Now I have nearly 270 new resources,” he said, “colleagues and friends who can help me solve the next problem, or maybe I can help them.”

Robert Ferrari, a lieutenant with the San Juan County Sheriff’s Office in Farmington, New Mexico, added, “Being from a small town in New Mexico, I was feeling that some of the issues in my organization—tight budgets, management challenges—were just our issues. But then you come here and find out that a guy from halfway across the world in Africa is having the same problems. The National Academy gives you the ability to network with all these people,” Ferrari said. “This experience has given me a lot of encouragement as a leader.”

**The program also emphasizes physical fitness, and students train with academy fitness instructors during their 10 weeks at Quantico to tackle the “Yellow Brick Road,” a grueling 6.1 mile run and obstacle course.** Upon completion of the course they receive a yellow brick to signify their accomplishment.

“Law enforcement only succeeds if we build global partnerships,” Kevin Perkins, the FBI’s associate deputy director, told this session’s graduates. “With every brick you earned here,” he said, “we are building that foundation.”

“Everybody who has participated in the National Academy, whether current students or past graduates—we all have an extreme sense of pride about being affiliated with the FBI,” Connolly said. “We aren’t agents, but we are now part of the fabric of the FBI. I think that’s important, that we have something tangible that connects us to the FBI.”

## Living a Lie

### Identity Theft That Lasted Decades

When Florida Highway Patrol Trooper Richard Blanco—a member of the FBI's Joint Terrorism Task Force (JTTF) in Jacksonville—interviewed an individual suspected of driver's license fraud in 2011, he wasn't initially sure if the man was the victim or the perpetrator of identity theft.

**That's because the man—now imprisoned and officially known as John Doe—had a stack of government-issued identification acquired during the 22 years he had been using a living victim's identity.** That included a passport, driver's license, birth certificate, Social Security card, and identification allowing him unescorted access to a port and military installation.

"He was extremely convincing that he was the victim," said Blanco, a veteran trooper with more than 30 years on the force. "When you have 20 forms of identification and it's in your possession," Blanco explained, "it's hard to not believe you are the person you say you are."

But John Doe was indeed an imposter, and while he was living under another man's name, the real victim was living a nightmare. It all started in 1989, when the victim's car was broken into and his wallet was stolen. His identity had been compromised.

John Doe began using the victim's name, even when he went to prison for aggravated battery. As a result, Blanco said, "if you run John Doe's fingerprints, even today, they will come back with the victim's name."

When the victim, a Miami resident, applied to become a corrections officer, he had to explain why his records showed a felony conviction. He urged officials to compare his fingerprints to those of John Doe's. When the victim applied for a passport, he was denied because the passport office claimed he already had one—the one that John Doe had applied for and received.

**When Blanco was able to talk with the real victim, he heard two decades worth of frustration.** The victim had filed a police report years before, but John Doe had never been caught or stopped. Blanco remembers the victim telling him, "This guy has been living my identity. He's gotten my license suspended, and he's had kids in my name."



When Blanco realized that he was dealing with a massive and long-running case of identity fraud, John Doe was arrested. The JTTF opened an investigation, and John Doe was eventually indicted federally on numerous counts of aggravated identity theft and fraud.

JTTF investigators had to rule out any threat to national security, because John Doe had access to the Mayport Naval Station as well as JaxPort, the Jacksonville Port Authority. Although he was just working at those locations, Special Agent Paxton Stelly, who supervises Jacksonville's JTTF, pointed out that John Doe had passed the background checks required to gain access there. "He appears to have manipulated the system with ease," Stelly said.

Last month, a jury convicted John Doe—who continues to insist he is the real victim in the case—and sentenced him to 10 years in prison. Despite DNA testing and a thorough investigation, his real identity remains a mystery.

"It will continue to be a mystery unless he makes an admission to us," Blanco said, adding, "I don't know what he's going to do when he gets out of prison, because the man doesn't have an identity."



Left: Ahmad Abousamra is wanted for supporting al Qaeda and seeking to kill U.S. soldiers.

## Help Us Catch a Terrorist

### U.S. Citizen Wanted for Supporting al Qaeda

The FBI today announced a reward of up to \$50,000 for information leading to the arrest of Ahmad Abousamra, a U.S. citizen from Massachusetts charged with traveling to Pakistan and Yemen to seek military training so he could kill American soldiers.

“Knowing that the public is the FBI’s best ally in finding fugitives, today we’re requesting your assistance to locate Abousamra,” said Richard DesLauriers, special agent in charge of our Boston office.

Abousamra is charged with conspiracy to provide material support or resources to al Qaeda. He was indicted in 2009 for taking multiple trips to Pakistan and Yemen in 2002 and 2004 to seek jihad training. He also traveled to Iraq with the hope of joining forces fighting against Americans overseas. Abousamra left the U.S. in 2006 and may be living in Aleppo, Syria with his wife, at least one daughter, and extended family.

Abousamra’s co-conspirator, Tarek Mehanna, was convicted of terrorism charges by a federal jury in December 2011 and sentenced last April to 17.5 years in prison.

“Both men were self-radicalized and used the Internet to educate themselves,” said Special Agent Heidi Williams, a member of our Joint Terrorism Task Force (JTTF) in Boston who has been working the case since 2006. “They came to it independently, but once they found each other, they encouraged each other’s beliefs,” Williams said,

adding that both Abousamra and Mehanna were inspired by the 9/11 terror attacks. “They celebrated it,” she said.

Abousamra is of Syrian descent and has dual U.S. and Syrian citizenship. He is 31 years old, 5’11” tall, and at the time of his disappearance weighed about 170 pounds. He has dark brown hair and brown eyes. He is fluent in English and Arabic, has a college degree related to computer technology, and was previously employed at a telecommunications company. Abousamra last lived in the U.S. in a prosperous Boston suburb and has family members in the Detroit, Michigan area.

One of his distinguishing characteristics is his higher-pitched voice, which can be heard on our website.

Today’s announcement is part of a publicity campaign employing traditional and social media to seek the public’s assistance. We are using social media to reach an overseas audience—information about Abousamra such as photos and audio clips can be found on the website and our Facebook, You Tube, and Twitter pages.

“Combining the reach and power of multiple media platforms is a powerful way to inform the public about our search,” DesLauriers said. “We believe publicizing Abousamra’s photo and characteristics will lead to a tip about his whereabouts and, ultimately, to his arrest.”

Thomas Daly, a sergeant with the Lowell Police Department in Massachusetts and a task force officer on the Boston JTTF since 2002, said catching Abousamra “will close the chapter on this story. We had two people who were planning to harm U.S. soldiers overseas,” Daly said, referring to Abousamra and Mehanna. “These two were actively radicalizing others. We can only assume Abousamra is still on the same path and remains a threat to our soldiers overseas.”

**We need your help.** If you have any information regarding Ahmad Abousamra, please contact your local FBI office or the nearest American Embassy or Consulate. You can also submit a tip electronically on our website at <https://tips.fbi.gov>.



Scan this QR code with your smartphone to watch a video on Abousamra, or visit <http://www.fbi.gov/news/videos/>.



# Distressed Homeowner Initiative

## Don't Let Mortgage Fraud Happen to You

Talk about going from bad to worse—more than 4,000 financially strapped homeowners recently lost at least \$7 million to a California business that allegedly operated a loan modification scam. Last month, 11 representatives of that company were federally indicted, but by that time, many of the victims had already lost their homes.

Today, to help protect distressed homeowners around the country from a rising tide of fraud schemes—and to raise awareness about them—the FBI joined the Department of Justice, the Department of Housing and Urban Development, and the Federal Trade Commission (FTC) in announcing the results of the Distressed Homeowner Initiative. This initiative was launched by the Bureau—co-chair of the Financial Fraud Enforcement Task Force's Mortgage Fraud Working Group—in October 2011.

This initiative combines the resources of federal, state, and local law enforcement agencies and the efforts of regulatory agencies to target perpetrators both criminally and civilly. Over 200 companies have been shut down, and criminal charges were filed against 530 defendants. These cases involved losses of more than \$1 billion from more than 73,000 victims across the country.

Said Associate Deputy Director Kevin Perkins, "In contrast with previous initiatives, where the fraud victims primarily were lenders, the focus here is on individual homeowners, many times at their most vulnerable point."

Based on intelligence from multiple sources, schemes targeting distressed homeowners have emerged throughout the country, and while the majority of FBI mortgage fraud cases involve loan origination fraud, we've had a 300 percent increase over the past three years in cases involving distressed homeowner fraud.

And with current mortgage data showing that 22.3 percent of residential properties with mortgages are "underwater"—when borrowers owe more than their homes are worth—we believe that fraudsters will certainly continue to target distressed homeowners.

We've also noticed a disturbing trend among these cases—an increasing number of lawyers playing primary or secondary roles in the fraud. In 2010, the



FBI Associate Deputy Director Kevin Perkins, right, is joined by Attorney General Eric Holder at a press conference announcing the results of the yearlong Distressed Homeowner Initiative.

FTC issued a rule that prohibited companies that offer loan modification or other types of mortgage assistance services from asking for fees in advance (some states have similar regulations), but with an exemption in some instances for lawyers performing legal work. Criminals targeting distressed homeowners try to circumvent the rules by using attorneys—which by itself adds an air of legitimacy to their fraudulent schemes—and calling their upfront fees "legal retainers."

The FBI's Financial Intelligence Center played a critical role at the outset of the initiative by reviewing and analyzing thousands of consumer complaints referred to us by our partners at the FTC, which helped identify where high-priority offenders were operating and allowed us to strategically deploy our investigative resources. The analysis of information from our partner agencies and from our own investigations will continue to be a vital part of our efforts to protect homeowners. The FBI also remains committed to targeting the most egregious criminal offenders with sophisticated investigative techniques—like undercover operations and court-authorized electronic surveillance—and through joint efforts with our law enforcement and regulatory partners.

If you have been victimized by those who claimed they could get you some kind of mortgage relief but didn't, please submit a tip to us online at <https://tips.fbi.gov> or contact your local FBI office.



Scan this QR code with your smartphone to watch a public service announcement featuring Tim DeKay of the television show *White Collar*, or visit <http://www.fbi.gov/news/videos/>.



## North to Alaska

### Part 1: Smallest FBI Office Takes on Big Job

The FBI recently investigated a white powder letter incident in Alaska with the help of a partner law enforcement agency. “It took our partners two days to get to the place where the white powder letter was,” said Mary Frances Rook, special agent in charge of our Anchorage Field Office, “because they had to take a ferry and a plane and an all-terrain vehicle to get to the school where the letter had been sent.”

**Welcome to the Anchorage Division—the FBI’s smallest field office—whose agents are responsible for covering the most territory of any office in the Bureau. That’s an area of more than 600,000 square miles, twice the size of Texas and packed with natural beauty and hard-to-reach places.**

Although the Anchorage Division investigates the same types of violent crime, public corruption, and national security matters as FBI offices in the Lower 48, “there is so much that is different here,” said Rook—and she’s not just referring to the bears and moose occasionally spotted on downtown Anchorage streets.

“If you’re in Anchorage, there are roads to Fairbanks and to the Kenai Peninsula, but other than that there are no roads,” Rook said. Getting to remote villages and towns requires a plane or a boat. Combine the geographical difficulties with extreme weather and one begins to understand how the 49th state can pose considerable challenges for the agents and support staff in Anchorage and our satellite locations in Fairbanks and Juneau.

**Left: In many cases, getting to remote Alaskan villages and towns requires a plane or a boat.**

Few FBI offices require snowmobiles to respond to crime scenes, but Anchorage keeps two on hand. The harsh Alaskan winters, where temperatures can plummet to more than 50 degrees below zero and the sun rises above the horizon for only a few hours each day, can make being outdoors seem almost otherworldly.

“It can be a challenging place to work,” Rook acknowledged. “But the flip side is that everybody knows it. So everybody works together. We work great with each other and with our local and federal law enforcement partners. Everybody’s got each other’s back, because you just can’t survive up here alone.”

**Not surprisingly, it takes a certain kind of person to work for the FBI in Alaska.** “The most successful Bureau people here are the ones who come with an idea that this is going to be a great adventure,” said Rook, whose assignment in Anchorage began in January 2011.

Special Agent Catherine Ruiz, who transferred to Anchorage with her husband last year from Chicago, agreed. “Every few days you will be driving home and you look up at the snowcapped mountains and say, ‘Wow, this is a beautiful place.’”

Bureau personnel who come to Alaska tend to be multi-talented as well. “We don’t have a lot of resources,” Rook said, “so everyone has to do a little bit of everything.” One of the office’s three pilots, for example, is also the polygraph examiner and a full-time counterintelligence agent. “That’s not unusual,” Rook noted.

“I originally thought I would come to Alaska for a few years,” said Special Agent Eric Gonzalez. That was 15 years ago. Gonzalez liked the place and the people—and so did his family. He added, “Most of the Bureau folks I know who worked here and left wished they would have stayed.”

*Part 2: An explosive situation in the dead of winter (page 86)*



Scan this QR code with your smartphone to watch a related video, or visit <http://www.fbi.gov/news/videos/>.

# Safe Online Surfing

## New Cyber Safety Website for Teachers, Students

With school back in session, one topic that's on many class curriculums around the nation is cyber safety. After all, it's a hyper-connected world—with texting, social networking, e-mail, online gaming, chat, music downloading, web surfing, and other forms of wired and wireless communication now a regular part of children's lives.

**The FBI has a new program that can help.** Today, as part of its longstanding crime prevention and public outreach efforts, the FBI is announcing a free web-based initiative designed to help teachers educate students about cyber safety.

**It's called the FBI-SOS (Safe Online Surfing) Internet Challenge**—and it was developed with the assistance of the National Center for Missing & Exploited Children and with the input of teachers and schools.

FBI-SOS is available through a newly revamped website at <https://sos.fbi.gov>. The site features six grade-specific “islands”—for third- through eighth-grade students—highlighting various aspects of cyber security through games, videos, and other interactive features. Each island has either seven or eight areas to explore—with a specific cyber safety lesson—and its own central character and visual theme. For example, fourth grade features Ice Island, complete with falling snow and penguins.

**To encourage participation and enhance learning, FBI-SOS includes both testing for students and competition among schools.** Each grade level has its own exam, which can only be taken after teachers have signed up their respective classes and all activities on the island have been completed by each student. And once all the exams for a class are graded (done electronically by the FBI), schools appear on a leader board in three categories based on the number of total participants. During each rating period, top-scoring schools in each category nationwide are awarded an FBI-SOS trophy and, when possible, receive a visit from a local FBI agent. All public, private, and home schools are eligible to participate.

For teachers and schools, FBI-SOS provides virtually everything needed to teach good cyber citizenship:

- A free, ready-made curriculum that meets state and federal Internet safety mandates;
- Age-appropriate content for each grade level;



The FBI-SOS site highlights cyber security through games, videos, and other interactive features.

- A printable teacher's guide that spells out how teachers can sign up their classes and use the site; and
- Detailed rules and instructions for students.

**Can anyone visit the website?** Absolutely. Kids of all ages—and even adults—can explore the site, play the games, watch the videos, and learn all about cyber safety. However, the exam can only be taken by third- to eighth-grade students whose classes have been registered by their teachers.

**An important note:** the FBI is **not** collecting student names, ages, or other identifying information through the website. Students are identified only by number when taking the exams; their teachers alone know which number matches which student. And teachers only need to provide their name, school, and e-mail address when signing up. The e-mail address is needed to verify the teacher's identity for registration purposes.

“FBI-SOS is a fun, free, and effective way to teach kids how to use the Internet safely and responsibly,” says Scott McMillion, head of the unit that manages the program in the FBI's Criminal Investigative Division. “We encourage teachers to check out the site and sign up their classes during the school year.”



Scan this QR code with your smartphone to watch a public service announcement on SOS, or visit <http://www.fbi.gov/news/videos/>.





## North to Alaska

### Part 2: An Explosive Situation in the Dead of Winter

The call came in to the Anchorage Field Office early on a Sunday morning in January 2010. An explosion had taken place at a Fairbanks residence, and a 21-year-old man had been seriously injured.

**After consulting with local authorities on the scene, our weapons of mass destruction (WMD) coordinator and other FBI personnel were not sure if the explosion was related to a drug manufacturing operation or linked to a terrorism threat.** But everyone understood that our assistance was required, because the house contained a variety of hazardous, unstable materials.

Members of our Evidence Response Team (ERT), the Joint Terrorism Task Force (JTTF), and others from the Anchorage office gathered their equipment and prepared to drive to Fairbanks—365 miles to the north—in the middle of a violent winter storm.

“It was 58 degrees below zero, with high winds, blizzard conditions, and black ice on the highway,” said Special Agent Derek Espeland, the WMD coordinator who is also one of Anchorage’s two special agent bomb technicians.

Based on the description of materials in the house, agents initially thought the man was making methamphetamine—meth labs are an unfortunate reality in many rural communities. The victim, who walked to a nearby fire station despite the sub-zero temperature, was burned and bleeding. He claimed he was building a rocket when it blew up. Before he could be questioned further, he was flown to a burn unit in Seattle for treatment.

---

**Left: The elements can present special challenges for investigators—in this case, bomb technicians.**

---

After a harrowing drive from Anchorage that took more than seven hours, FBI personnel arrived on scene along with bomb techs from the Air Force and local law enforcement. The meth lab theory was ruled out, “but then you almost had to conclude that the guy could be a terrorist,” Espeland said. “Everything we saw in the house we had seen being used by terrorists in Iraq and Afghanistan.”

As it turns out, the 21-year-old was neither a drug maker nor a terrorist. He was just fascinated with explosives and blowing things up. He had legally purchased all his ingredients—of course, our agents didn’t know that at the time. And because the house was a public safety threat, Espeland said, “we couldn’t just walk away.”

**To neutralize the threat, it was decided to employ several render-safe techniques using specialized equipment.** But that was easier said than done. Robots and other battery-powered equipment were inoperable in the nearly 60-below temperature because the batteries were frozen. Espeland’s evidence camera froze to his face when he tried to take a picture—inside the house. Vehicles had to be kept running for fear they would freeze if turned off, even with warming blankets and engine block heaters. An extension cord designed for extreme cold snapped and disintegrated.

“The cold was drier than anything I ever felt before,” said Vicky Grimes, an ERT member. “It almost took your breath away.”

A command post was established at the nearby fire station, and after a joint effort, the house was finally rendered safe. “Responding to this incident reinforced our understanding that we have to rely on our state and local partners for assistance, just as they rely on us,” said Special Agent Sandra Klein, Anchorage’s JTTF supervisor.

The 21-year-old recovered from his injuries, and—since he had committed no federal crimes—was not charged. “This was a public safety threat that could have been something far more serious,” Espeland said. “That’s why we responded, despite the conditions. That’s what we’re here for.”

*Part 3: A domestic terrorist with a deadly plan (page 92)*

# Remembering Lou Peters

## Selfless Actions Brought Down Mob Boss

In 1977, things were going well for Lou Peters—he was living the American dream with his wife and three daughters, running a successful Cadillac dealership in Lodi, California. And in June of that year, he got an offer he couldn't refuse.

A man approached Peters expressing interest in buying the dealership. When told it wasn't for sale, the man was insistent, telling Peters to "name any price." Finally, Peters said he would sell it for \$2 million—nearly twice what the business was worth. The man accepted—then told Peters that the buyer was none other than Joseph Bonnano, Sr., head of the Bonnano organized crime family, who wanted the dealership to launder the family's illegal funds.

**Initially taken aback upon learning of mafia involvement, Peters eventually agreed to the sale,** recounting, "I didn't understand why these people wanted to come into our county. And I wanted to find out." He then went to a local police chief and told him what had happened. When the chief asked what he was going to do next, Peters replied, "Well, I'm going to the FBI."

And to the FBI he went, telling all. The FBI saw an opportunity to take down Bonnano and asked Peters for help. He was on board. "I felt it was the right thing to do, and I just did it," he said.

**Over the next nearly two years, Peters played the part of a corrupt businessman, gaining remarkable access to the Bonnano family and even becoming a close companion of Joseph Bonnano, Sr.** To gain his confidence, Peters recalled saying something to "the old man" along the lines of, "Well, this should really bring me into the family"—to which Bonnano replied, "Lou, you're already in the family."

Through it all, Peters never took his eye off the ball—gathering evidence, secretly recording conversations, and debriefing agents on what he had learned. And his efforts weren't without personal sacrifice...besides the risk to his life, he had to obtain a (temporary) legal separation from his wife not only to protect his family but also to have a credible reason to move out of his house—and into an apartment that was being monitored by the FBI.



In National Archives footage, Lou Peters talks about his role in the FBI's case against the head of the Bonnano organized crime family.

**In the end, Peters got what we needed.** When he told Bonnano—during a recorded call—that he had been subpoenaed to testify before a grand jury regarding his dealings with the family, the old man directed him to destroy any records that could be linked back to him and his associates. Peters took the tape to the FBI agent on the case. While listening to it, the agent jumped up and said, "You got him!"

Thanks to Lou Peters, Joseph Bonnano, Sr. was found guilty of obstructing justice and sentenced to five years in prison—the first felony conviction in the mob boss' long life of crime.

To show its appreciation, in October 1980 the FBI presented Peters with an award for his selfless and valiant actions...an award that has been granted annually for the past 30 years as the Louis E. Peters Memorial Service Award, bestowed upon the citizen who best exemplifies the standards set by Peters in providing service to the FBI and the nation.

Shortly before his death in 1981, Peters said, "I was very proud of what I did for my country." The country is very proud of him, too. Thanks, Lou Peters.



Scan this QR code with your smartphone to watch a video interview of Lou Peters, or visit <http://www.fbi.gov/news/videos/>.



## Cyber Security

### Focusing on Hackers and Intrusions

Early last year, hackers were discovered embedding malicious software in two million computers, opening a virtual door for criminals to rifle through users' valuable personal and financial information. Last fall, an overseas crime ring was shut down after infecting four million computers, including half a million in the U.S. In recent months, some of the biggest companies and organizations in the U.S. have been working overtime to fend off continuous intrusion attacks aimed at their networks.

The scope and enormity of the threat—not just to private industry but also to the country's heavily networked critical infrastructure—was spelled out last month in Director Robert S. Mueller's testimony to a Senate homeland security panel: "Computer intrusions and network attacks are the greatest cyber threat to our national security."

To that end, the FBI over the past year has put in place an initiative to uncover and investigate web-based intrusion attacks and develop a cadre of specially trained computer scientists able to extract hackers' digital signatures from mountains of malicious code. Agents are cultivating cyber-oriented relationships with the technical leads at financial, business, transportation, and other critical infrastructures on their beats.

Today, investigators in the field can send their findings to specialists in the FBI Cyber Division's Cyber Watch command at Headquarters, who can look for patterns or similarities in cases. The 24/7 post also shares the information with partner intelligence and law enforcement agencies—like the Departments of Defense and

Homeland Security and the National Security Agency—on the FBI-led National Cyber Investigative Joint Task Force.

A key aim of the Next Generation Cyber Initiative has been to expand our ability to quickly define "the attribution piece" of a cyber attack to help determine an appropriate response, said Richard McFeely, executive assistant director of the Bureau's Criminal, Cyber, Response, and Services Branch. "The attribution piece is: who is conducting the attack or the exploitation and what is their motive," McFeely explained. "In order to get to that, we've got to do all the necessary analysis to determine who is at the other end of the keyboard perpetrating these actions."

The Cyber Division's main focus now is on cyber intrusions, working closely with the Bureau's Counterterrorism and Counterintelligence Divisions.

**"We are obviously concerned with terrorists using the Internet to conduct these types of attacks,"** McFeely said. **"As the lead domestic intelligence agency within the United States, it's our job to make sure that businesses' and the nation's secrets don't fall into the hands of adversaries."**



Executive Assistant Director  
Richard McFeely

In the Coreflood case in early 2011, hackers enlisted a botnet—a network of infected computers—to do their dirty work. McFeely urged everyone connected to the Internet to be vigilant against computer viruses and malicious code, lest they become victims or unwitting pawns in a hacker or web-savvy terrorist's malevolent scheme.

**"It's important that everybody understands that if you have a computer that is outward-facing—that is connected to the web—that your computer is at some point going to be under attack,"** he said. **"You need to be aware of the threat, and you need to take it seriously."**



## Latest Crime Stats

### Annual Crime in the U.S. Report Released

According to our just-released *Crime in the United States, 2011* report, the estimated number of violent crimes reported to law enforcement (1,203,564) decreased for the fifth year in a row, while the estimated number of property crimes reported to law enforcement (9,063,173) decreased for the ninth year in a row.

You can access the full report on our website, but here are a few highlights:

#### Violent Crime

- The South, the most populous region in the country, accounted for 41.3 percent of all violent crimes (lesser volumes of 22.9 percent were attributed in the West, 19.5 percent in the Midwest, and 16.2 percent in the Northeast).
- Aggravated assaults accounted for the highest number of estimated violent crimes reported to law enforcement at 62.4 percent.
- Firearms were used in 67.8 percent of the nation's murders, 41.3 percent of robberies, and 21.2 percent of aggravated assaults (data on weapons used during forcible rapes is not collected).
- In 2011, 64.8 percent of murder offenses, 41.2 percent of forcible rape offenses, 28.7 percent of robbery offenses, and 56.9 percent of aggravated assault offenses were "cleared"—either by the arrest of the subject or because law enforcement encountered a circumstance beyond its control that prohibited an arrest (i.e., death of the subject).

#### Property Crime

- 43.2 percent of the estimated property crimes occurred in the South (followed by the West with 22.8 percent, the Midwest with 21.1 percent, and the Northeast with 13 percent).
- Larceny-theft accounted for 68 percent of all property crimes in 2011.
- Property crimes resulted in losses of \$156.6 billion.
- Also cleared were 21.5 percent of larceny-theft offenses, 12.7 percent of burglary offenses, 11.9 percent of motor vehicle theft offenses, and 18.8 percent of arson offenses.



The FBI's Uniform Crime Reporting (UCR) program is one of two statistical programs administered by the Department of Justice that measure the magnitude, nature, and impact of crime—the other is the National Crime Victimization Survey (NCVS), conducted by the Bureau of Justice Statistics.

Both were designed to complement each other, providing valuable information about aspects of the nation's crime problem, but users should not compare crime trends between the two programs because of methodology and crime coverage differences. The UCR program provides a reliable set of criminal justice statistics for law enforcement administration, operation, and management, as well as to indicate fluctuations in the level of crime, while the NCVS provides previously unavailable information about victims, offenders, and crime...including crimes not reported to police. Additional information about the differences between the two programs can be found in the *Nation's Two Crime Measures* section of *Crime in the United States*.

Looking ahead to 2013 and beyond, the UCR program is working to complete the automation of its data collection system, which will result in improved data collection efforts with new offense categories and revised offense definitions...as well as a faster turnaround time to analyze and publish the data. And beginning with the 2013 data, the new definition for rape will take effect—the FBI is developing options for law enforcement agencies to meet this requirement, which will be built into the new data collection system.

UCR's *Law Enforcement Officers Killed and Assaulted, 2011* and *Hate Crimes Statistics, 2011* will be available on our website later this fall.



Left: The families of fallen agents Robin Ahrens and Martha Dixon Martinez were given memorial plaques at a recent meeting of the Society of Former Special Agents of the FBI.

## Celebrating Women Special Agents

### Part 7: Two Have Made the Ultimate Sacrifice

With eight kids under the roof, the Dixons' one-bathroom house in Pittsburgh had no room for the mitts, hockey sticks, and other accoutrements of active all-weather children. So everything was kept on the front porch. When things went missing, nobody was surprised when Martha, the sixth child and a future FBI special agent, initiated her own stake-out, sleeping on the porch and nabbing the culprit red-handed. It was the paperboy.

"That to me was probably the most revealing thing in her childhood of a law enforcement personality," said Monica Dixon Dentino, Martha's younger sister. "For her to say, 'Yep, I'm going to sleep by myself on the front porch to confront somebody that's invading our house'—she was tough like that."

Many years later, in 1994, when a gunman began shooting in a squad room at the Metropolitan Police Department in Washington, D.C., Martha Dixon Martinez apparently chose to confront the attacker rather than retreat. She and fellow Special Agent Michael John Miller were killed in the exchange, along with a D.C. police officer.

The event, recounted by Martha's two sisters at a recent convention of former special agents recognizing the 40-year anniversary of women agents, marked the second time in the Bureau's history that a woman agent was killed in the line of duty. Nine years earlier, in 1985, Special Agent Robin L. Ahrens was killed in Phoenix during an operation to arrest an armed robber. Both agents' stories—the last part of our series marking

four decades of women agents—punctuate how a desire to serve has led women from all backgrounds to become special agents since the position opened to women in 1972.

"You couldn't tell her not to do that job because we worry about you," said Christian Ahrens, one of Robin's four brothers. "She would just go forage forward. That's [the decision] she made—to be a special agent. I wish I could go back and say, 'Be careful. Watch your back.' But that's not possible."

Born in St. Paul, Minnesota, Robin was one of six kids who thrived outdoors, volunteering as a teenager on the National Ski Patrol. As a school teacher in Virginia, she led a field trip to the U.S. Marine base at Quantico—home to the FBI Training Academy—and decided what she wanted to do. She became an agent in June 1985; just four months later, she was killed.



Robin Ahrens and Martha Dixon Martinez

"It was a tragic event," said James Ahrens, Robin's older brother. "But when she was joining the FBI, she was excited. She was so happy to be in. I keep looking at that part of it, too."

While Robin's path to the FBI seemed serendipitous, Martha Dixon's journey appeared preordained. A chemistry major in college, she worked in the lab of a local hospital, determined to one day work at the FBI Laboratory. She became an agent in 1987 and quickly discovered in her first office in Knoxville that she preferred working on the front lines. "She liked solving the problems and closing a case," her sister Monica said.

Martha transferred to the Washington Field Office, where she went to work on a cold case homicide squad. On November, 22, 1994, a gunman passed her by as he entered the squad room at police headquarters, possibly mistaking her for a secretary. Then came the shots.

"She heard the noise and chose not to leave," said Jan Dixon Smith, Martha's older sister. "She went in. She just knew that she might be able to do something. And that makes us very proud."

# Operation Universal Money Fast

## Putting the Brakes on Health Care Fraud

With its aging, affluent population, South Florida is ground zero for the multi-billion-dollar criminal industry of health care fraud. Few cases illustrate the depth of the problem—and our efforts to fight it—more than Operation Universal Money Fast.

The case involved a massive, sophisticated fraud against Medicare and private insurance companies by scammers who set up more than a dozen fake clinics across five states and submitted tens of millions of dollars in bogus claims related primarily to HIV infusion therapy.

Using stolen identities and bribing physicians to lend an air of legitimacy to the fraud, the thieves bilked the system for an estimated \$70 million before we dismantled the enterprise.

Despite the many safeguards built into the Medicare reimbursement process—such as audits and on-site visits to clinics and providers—the system is largely based on trust. If a business believed to be legitimate submits claims using proper paperwork and billing codes, those claims are paid quickly.

The crooks were counting on that. They knew the fraud would eventually be discovered, but they stayed one step ahead of authorities by opening shell companies and phantom clinics across Florida, Georgia, Louisiana, North Carolina, and South Carolina. In reality, the clinics were empty storefronts—some were nothing more than a post-office box. No patients were ever seen or treated, and no doctors worked there.

“All they needed was a laptop, stolen identities, and billing codes,” said Special Agent Randy Culp, who works health care fraud investigations out of our Miami office. “By the time the insurance companies suspected fraud, the fraudsters had already moved on to some new fictitious clinic.”

To conceal their true identities, the subjects registered the bogus businesses in the names of nominal owners and opened a check-cashing store—called Universal Money Fast—to launder more than \$50 million in benefits paid by Medicare and private insurers.



Ramon Fonseca, Orlin M. Tamayo Quinonez, and Juan Carralero are wanted for allegedly conspiring in a scheme to defraud the Medicare program out of tens of millions of dollars.

“Insurance companies were alerted by their customers to the fraud,” Culp said. “People were getting statements and seeing benefits for infusion therapy, and they were calling and saying, ‘Hey, I’m not HIV-positive. What’s going on?’”

During the height of the scam, said Special Agent Liz Santamaria, who worked on the case, “the subjects were submitting Medicare bills at the rate of \$100,000 per week. They were making easy money and spending it as soon as they made it,” she added, explaining that the scammers thought nothing of dropping \$10,000 in one evening for a lavish dinner.

Our Medicare Fraud Strike Force opened an investigation in 2009 and used investigative tools such as sources and search warrants to stop the fraud and arrest the perpetrators. In 2010, ringleader Michel De Jesus Huarte received a record sentence for health care fraud of 22 years in prison. Nine other defendants received significant sentences as well. Three remaining subjects in the case remain at large and are believed to be out of the country.

“Large-scale fraud like this undermines the financial integrity of the Medicare program,” Culp said. “The FBI and our partners are committed to fighting these white-collar criminal enterprises, and we are gratified that those who commit these frauds are getting significant prison terms for their actions.”





Left: Paul Rockwood, seen here in a surveillance image, lived in the small fishing village of King Salmon. He had begun compiling a list of targets in the U.S. military he might assassinate in the name of jihad.

## North to Alaska

### Part 3: A Domestic Terrorist with a Deadly Plan

By the time he moved to Alaska in 2006, Paul Rockwood, Jr. was an ardent follower of the American-born radical cleric Anwar al-Awlaki, who he met at a Virginia mosque in late 2001.

**Shortly after he settled with his family in the small fishing village of King Salmon to work for the National Weather Service, our agents in Anchorage were aware that Rockwood had begun compiling a list of targets in the U.S. military he might assassinate in the name of jihad.**

“If you were wearing a U.S. military uniform,” said Special Agent Doug Klein, who worked the case from Anchorage, “as far as Rockwood was concerned, you were a target.”

A military veteran himself, Rockwood believed it was his religious duty to kill those who desecrated Islam. In 2009, he began sharing his deadly plans with an individual he thought held similar views. But that person was actually an undercover operative employed by our Joint Terrorism Task Force (JTTF) in Anchorage.

For a time, JTTF personnel wondered how determined Rockwood was about his plans. “But one day when he was with our undercover in Anchorage, he identified the building of a cleared defense contractor and said, ‘This is the kind of building I want to blow up,’” Klein said. “That’s when we knew he was a serious threat.”

Keeping track of Rockwood was difficult, however, because King Salmon is some 300 miles from Anchorage and only accessible by airplane. And with only a few hundred residents, outsiders would be immediately

spotted, so attempts at surveillance were impractical. “We couldn’t use 90 percent of the traditional investigative techniques we use in the Lower 48,” Klein explained.

In addition, small, regional airlines in Alaska are not regulated by the Transportation Security Administration, so anyone can fly with weapons. On Rockwood’s frequent trips from King Salmon to Anchorage, Klein said, “he could have had a gun or a bomb and we never would have known.”

**During those Anchorage visits, Rockwood met the undercover operative and discussed buying electronics and downloading schematics of cell phones to make bomb detonators.** At one meeting, he said he was getting ready to relocate to the mainland and had plans to steal a cache of explosives in Boston—where he grew up—that would help him go operational.

By early 2010, Rockwood had formalized his hit list to include 15 specific targets—all outside Alaska—and he gave the list to his wife, Nadia, who was aware of his intentions.

Even with no overt acts of terrorism to charge him with, it was decided that for the sake of public safety, Rockwood could not be allowed to leave Alaska. In May 2010, JTTF agents questioned Rockwood and his wife as they attempted to fly out of Anchorage. Both denied any involvement with a hit list or terrorist plot.

The couple was charged with making false statements to the FBI in a domestic terrorism investigation, and in July, Rockwood was found guilty and sentenced to eight years in prison—the maximum sentence under the law. His wife was also found guilty and received five years of probation.

“We can never be sure if he would have acted,” Klein said, “but Rockwood was clearly a threat, not only to the individuals on his list but to the entire community.”

*Part 4: The shot that pierced the Trans-Alaska Pipeline (page 96)*

# Two Most Wanted Terrorists Named

## Third Man Sought for Questioning

Two individuals—one a United States citizen who allegedly provided support to a foreign terrorist organization, the other wanted for his alleged role in the overseas kidnapping of an American—have been added to the FBI's Most Wanted Terrorists list.

A third man wanted for questioning in connection with providing material support to terrorists has been added to our Seeking Information—Terrorism list.

### Most Wanted Terrorists

Omar Shafik Hammami, formerly from Alabama, has reportedly been a senior leader in al Shabaab, an insurgency group in Somalia. Al Shabaab was designated a foreign terrorist organization by the U.S. State Department in 2008; it has since repeatedly threatened terrorist actions against America and American interests. Hammami allegedly traveled to Somalia in 2006 and joined al Shabaab's military wing, eventually becoming a leader in the organization. Hammami—who has been indicted in the U.S. on various terrorism charges—is believed to be in Somalia.

Raddulan Sahiron, a native of the Philippines, is wanted for his alleged involvement in the 1993 kidnapping of an American in the Philippines by the Abu Sayyaf Group, designated a foreign terrorist organization in 1997. Sahiron, believed to be the leader of the Abu Sayyaf Group, was indicted on federal hostage-taking charges and may currently be in the area of Patikul Jolo, Sulu, Philippines.

### Seeking Information—Terrorism

Shaykh Aminullah is wanted for questioning in connection with providing material support to terrorists...with the aid of Pakistan-based Lashkar-e-Tayyiba (designated a foreign terrorist organization in 2001). Among other activities, Aminullah allegedly provided assistance, including funding and recruits, to the al Qaeda network; provided funding and other resources, including explosive vests, to the Taliban; and facilitated the activities of anti-coalition militants operating in Afghanistan by raising money in support of terrorist activities. He is believed to be in the Ganj District of Peshawar, Pakistan.



Omar Shafik Hammami (left) and Raddulan Sahiron

The FBI's Most Wanted Terrorists list was created in October 2001. We subsequently created the Seeking Information—Terrorism list to publicize our efforts to locate terrorism suspects not yet indicted in the U.S.

In addition to the beneficial aspect of worldwide publicity, individuals named to the Most Wanted Terrorists list must:

- Have threatened the security of U.S. nationals or U.S. national security;
- Be considered a dangerous menace to society;
- Have indicated a willingness to commit or indicate to commit an act to cause death or serious bodily injury, prepare or plan terrorist activity, gather information on potential targets for terrorist activity, or solicit funds or other things of value for terrorist activity;
- Have provided material support such as currency or financial services or assistance to a terrorist organization but do not necessarily have to belong to that organization;
- Be subject to lawful detention, either by the U.S. government based on an active federal warrant for a serious felony offense or by any other lawful authority; and
- Be the subject of a pending FBI investigation.

Individuals on the Seeking Information—Terrorism list are being sought for questioning in connection with terrorist threats against the United States. Unlike those on the Most Wanted Terrorists list, these individuals have not been indicted by the U.S. government.

If you have information about any of these men, please submit a tip at <https://tips.fbi.gov> or contact the nearest FBI office abroad or in the United States.



## LCD Price Fixing Conspiracy

### Taiwanese Company, Execs Sentenced

Did you buy a computer notebook, computer monitor, or big-screen TV anytime from late 2001 to 2006? If you did, odds are that you paid too much for it because of an international criminal conspiracy to fix the prices of the LCD (liquid crystal display) panels used in these products.

Recently, AU Optronics Corporation—the largest Taiwanese producer and seller of LCD panels—and two of its former top executives were sentenced for their roles in this conspiracy. The company was ordered to pay a \$500 million criminal fine, and the executives each received three years in federal prison. AU Optronics is the eighth company convicted as a result of a joint FBI-Department of Justice (DOJ) Antitrust Division effort to uncover this worldwide price-fixing conspiracy.

**Anatomy of a conspiracy.** A few days after the terrorist attacks of 9/11, top-level executives from a number of Asian manufacturers of LCD panels met secretly in a Taiwan hotel room and agreed to a plan to fix the prices of LCDs in the U.S. and elsewhere.

During subsequent monthly meetings, group members exchanged production, shipping, supply, demand, and pricing information on LCD panels used in computer notebooks, monitors, and flat-screen TVs. Participants agreed on prices and would then sell their products at these prices to some of the world's largest technology companies who used LCD panels in their products.

During the same time period, senior-level employees of AU Optronics Corp. regularly exchanged information with its Houston-based subsidiary—AU Optronics Corp. America—on sales of LCD panels for the purpose of monitoring and enforcing adherence to the prices agreed upon by other LCD manufacturers in the U.S.

The end result of all this price-fixing? Artificially inflated prices for consumers, and more money into the coffers of the conspiracy's participants.

**Change in tactics.** These meetings went on until mid-2005, when participants learned that one or two of their major LCD customers may have become aware of the conspiracy, so the top leaders who had been attending these meetings began sending lower-level employees. The meetings were also moved out of hotel rooms and into public restaurants and cafes.

And a year later, the co-conspirators became even more concerned when they heard about an ongoing price-fixing investigation in the U.S. into the dynamic random access memory (DRAM) industry. To avoid detection, group members decided to meet one-on-one with each other in restaurants and cafes.

The FBI became involved in the case in mid-2006 at the request of DOJ's Antitrust Division, and Bureau investigators joined forces with Antitrust Division prosecutors. In antitrust cases, as in many of our white-collar crime cases, the FBI uses its full arsenal of investigative weapons—executing search warrants, interviewing witnesses and others, analyzing records, conducting lawful surveillance, using cooperating witnesses, etc.

**Additional sanctions.** In addition to the extraordinary criminal fine levied on AU Optronics and the sentencing of two former executives, the company was also ordered to implement an internal compliance program, hire an independent corporate compliance monitor, and take out ads in U.S. and Taiwanese newspapers publicizing the criminal sanctions taken against it.

These actions send a powerful message to would-be perpetrators of price-fixing and other antitrust schemes—the U.S. criminal justice system will uncover your illegal activities and hold you accountable.



# Making the Ultimate Sacrifice

## Report on Law Enforcement Officer Deaths Released

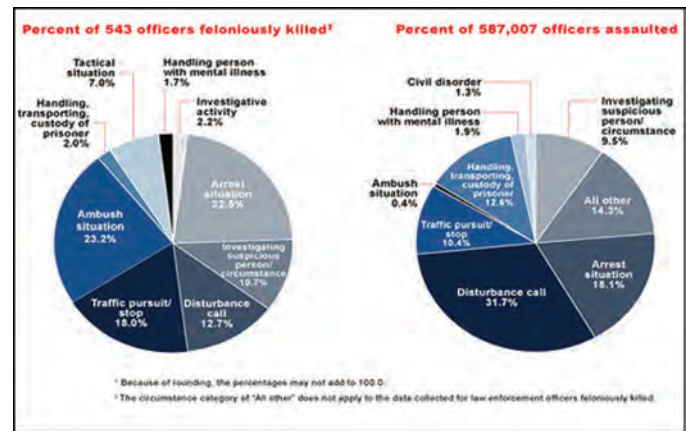
Tragically, during 2011, 72 law enforcement officers from around the nation were killed in the line of duty, while another 53 officers died in accidents while performing their duties. And 54,774 officers were assaulted in the line of duty...all according to our just-released annual report *Law Enforcement Officers Killed and Assaulted, 2011*.

Here's a look at some of the data collected for this report:

- While the 72 officers killed in the line of duty came from city, university and college, county, state, tribal, and federal agencies, the majority (50) were employed by city police departments.
- The average age of the officers feloniously killed was 38, while their average length of service was 12 years. Forty-nine of these officers were slain while on assigned vehicle patrol.
- Most of the 72 officers slain were killed with firearms, and 51 of these officers were wearing body armor at the time of their murders.
- Of the 53 officers who died accidentally, 39 were killed as a result of vehicle-related accidents.
- The rate of officer assaults in 2011 was 10.2 per 100 sworn officers.

Our *Law Enforcement Officers Killed and Assaulted* (LEOKA) report is intended to provide law enforcement agencies with detailed descriptions of circumstances leading to officer fatalities. This data can then be incorporated into police training programs to help officers stay safe during similar situations.

The primary goal of our overall LEOKA program is to reduce incidents of law enforcement deaths and assaults. In addition to its annual report, the program also offers an officer safety awareness training course that provides potentially life-saving information to help law enforcement personnel enhance their situational awareness during activities like arrests, traffic stops, foot pursuits, ambushes, and other high-risk encounters that police face on a daily basis.



Beyond services provided by the LEOKA program, the FBI offers additional training initiatives geared toward officer safety to our law enforcement partners.

For example:

- Our one-week Law Enforcement Training for Safety and Survival program at the FBI Academy is designed to teach participants basic survival techniques as well as the skills and mindset required to identify and handle critical situations in high-risk environments (i.e., arrests, low light operations, ballistic shield deployment).
- Our National Academy curriculum includes a communications course for law enforcement leaders on how to incorporate measures into their policies that will help ensure the future emotional well-being of officers who have survived shootings (as well as officers who have shot suspects).

In addition to the above training, the FBI's National Crime Information Center (NCIC)—accessed by more than 92,000 agencies—offers a measure of protection for law enforcement as well, particularly through its recently added Violent Persons File. Once fully populated with data from our users, a quick response from an online NCIC query can warn officers on the spot if, during a routine traffic stop or another type of encounter, they come across an individual who has a violent criminal history or who has previously threatened law enforcement.

The release of this latest LEOKA report clearly demonstrates what we already know—despite the dangers of law enforcement, the profession continues to attract brave men and women willing to make the ultimate sacrifice to protect their fellow citizens.



**Left:** In 2001, a resident of Livengood, Alaska—a town of less than two dozen people about 50 miles north of Fairbanks—shot a hole in the pipeline with a high-powered rifle.

## North to Alaska

### Part 4: The Shot That Pierced the Trans-Alaska Pipeline

Located less than 200 miles from the Arctic Circle, our resident agency in Fairbanks is one of the FBI's most remote offices—but its three investigators cover an expansive amount of territory and help safeguard some of the country's most valuable infrastructure.

Within the office's area of responsibility is the Trans-Alaska Pipeline, an 800-mile engineering marvel that has carried billions of gallons of crude oil from Prudhoe Bay to Valdez since it began pumping in 1977.

"For as long and as exposed as the pipeline is, it is definitely not a soft target on the ground or in the air," said Special Agent Bruce Milne. That's because the pipeline's owner, Alyeska Pipeline Service Company, provides extensive security and maintains strong ties with local and federal law enforcement.

"We all take the security of the pipeline very seriously," said Milne, a 25-year FBI veteran who was drawn to Alaska in part because of his interest in dog sledding. "Our Joint Terrorism Task Force coordinates closely with Alyeska and Alaska State Troopers to protect the pipeline," he added.

One case that stands out for Milne occurred in October 2001, when a resident of Livengood—a town of less than two dozen people about 50 miles north of Fairbanks—shot a hole in the pipeline with a high-powered rifle.

A bullet would not ordinarily breach the pipeline's exterior, which is constructed of thick steel and lined

inside with several inches of high-density insulation. But the single shot from Daniel Lewis' rifle somehow did penetrate the pipeline, and oil began streaming out with tremendous force. "If you would have put your hand in front of the leak," Milne said, "the pressure would have taken it off."

Lewis, described later in court as a career criminal, had been released from jail only weeks before the shooting incident. He was detained by troopers after he and his brother were spotted near the spill.

Milne and his colleague, Special Agent Mark Terra, were called in to investigate. They recovered the rifle—the scope had blood on it where it had recoiled against Lewis' face—made plaster foot casts at the crime scene, and began interviewing people who knew the Lewis brothers. "Alyeska security and local troopers did a tremendous amount of work on this case as well," Milne said.

**Meanwhile, oil spewed from the pipeline for days before engineers could stop it. More than 285,000 gallons of crude were spilled as a result of that small bullet hole and—according to press reports at the time—the cleanup took many months and cost \$13 million.**

Lewis was charged with a range of federal and state crimes, from weapons offenses to oil pollution, criminal mischief, and driving while intoxicated. In 2002 he received a 10-year federal sentence; the following year in state court, he was sentenced to 16 years in prison. His sentences are running concurrently.

Coming less than a month after the 9/11 terror attacks, the pipeline shooting served as a reminder that protecting the country—whether from terrorists or other criminals—requires constant vigilance. "Everyone here recognizes that the stakes are as high in Alaska as anywhere else," Milne said. "That's why we work so closely with our partners to maintain the highest level of security."

# Counterintelligence Awareness

## Teaching Industry How to Protect Trade Secrets and National Security

The FBI vigilantly investigates cases of industrial espionage and theft of intellectual property, but the Bureau also places great emphasis on preventing such crimes by educating industry on ways to keep trade secrets safe. One such innovative program in North Carolina's Research Triangle is a collaborative effort with other federal partners called RED DART.

**The threat to America's trade secrets—and to our national security—is real, whether it comes in the form of international spies, hackers probing online security systems, or disgruntled employees out for revenge.** RED DART seeks to mitigate the threat by raising counterintelligence awareness.

Through briefings to cleared defense contractors and others in technology-rich North Carolina, RED DART makes executives and employees aware of how counterintelligence works and how they can spot suspicious activity both inside and outside their companies.

"Everybody wants to emulate U.S. technology," said Brent Underwood, a special agent with the Naval Criminal Investigative Service who helped create RED DART. "If countries can shortcut 10 or 20 years' worth of research and development by stealing our technology, that puts them at an obvious advantage."

Despite the occasional high-profile case where a spy accesses highly classified documents, the majority of stolen technology is unclassified, said FBI Special Agent Lou Velasco, who manages the program out of our Charlotte Division. "With the right amount of information," he explained, "state actors can reverse-engineer our products or build them from scratch."

When that happens, our adversaries can be more competitive on the battlefield as well as in the global marketplace. "A big part of our program is putting information out there about the threat so that people understand just how serious it is," Velasco said. "When a company's trade secrets are compromised, it can threaten national security, but it can also hurt that company's bottom line and its ability to keep people employed."



The threat from inside a company may be employees secretly sent by foreign countries to steal secrets. RED DART briefings help employees spot suspicious behavior, such as a staffer working odd hours, asking inappropriate questions, or making frequent trips overseas. Externally, foreign agents may pose as potential investors or customers to gain access to technical information that could compromise a company's trade secrets. And weak online security is always an invitation to hackers.

Griff Kundahl, executive director of the Center of Innovation for Nanobiotechnology in North Carolina, a state-funded organization that fosters new technology in the region, has worked closely with the RED DART program to help educate the center's members.

"Our core constituents are early-stage companies," Kundahl said. "They developed a product that might treat cancer, for example. They are trying to raise money and get their product to market. They don't have much time or the resources to consider security risks. If RED DART can get them to understand these risks, it helps everybody. When they realize that all their efforts could be for naught if their technology is stolen or compromised, it can be eye-opening for them."

"Our challenge is to show how real the threat is," Velasco said. "We arm people with tools so that they can make appropriate business decisions."

Michelle Brody, a special agent with the Defense Security Service and a founding member of RED DART, added, "When RED DART helps a company protect itself a little better, it not only helps them, it helps our national security."





## Preying on the Weak

### Estate Planner Victimized Terminally Ill

It was a despicable scheme—stealing identities of terminally ill individuals to fraudulently obtain millions of dollars from insurance companies and bond issuers.

Attorney Joseph Caramadre, president and CEO of his own estate planning company in Rhode Island—along with Raymour Radhakrishnan, an employee—pled guilty earlier this month in federal court to conspiracy to commit identity theft and wire fraud.

**Caramadre's investment strategies depended on lying to terminally ill individuals and their loved ones to obtain identity information.** He abused two financial instruments—variable annuities and death put bonds—to carry out these strategies. In addition to buying annuities from insurance companies listing terminally ill individuals as annuitants, he also purchased bonds of distressed companies for significantly below face value listing terminally ill individuals as “co-owners.” When the terminally ill person died days or weeks later, he would exercise the death benefits associated with the investments.

Caramadre recruited investors by falsely telling them he found a loophole that permitted the use of terminally ill patients as annuitants on annuities and co-owners on brokerage accounts used to purchase death put bonds. He then entered into profit-sharing agreements with them, but received a significant percentage of the profits himself.

In recruiting terminally ill individuals for his scheme, Caramadre was only interested in those with a life expectancy of six months or less. He looked for victims

in several ways: visiting AIDS facilities, putting ads in a local religious newspaper offering cash to terminally ill individuals, and even looking through his own company files.

The ads purchased by Caramadre were especially fruitful...in them, he claimed to be a philanthropist and offered the terminally ill a few thousand dollars to assist with their funeral expenses. The ads also got him access to hospice care facilities, nurses, and social workers who could spread the word about his offer.

Radhakrishnan would visit patients and their families to supposedly determine whether they qualified for the donation, but he was actually assessing their life expectancies...the shorter the time, the better for the scheme.

Patients who accepted Caramadre's cash offer were asked to sign a document, ostensibly because the philanthropist needed it for tax records, but in reality it was so their signatures could be forged later on. Sometimes, they were asked to sign signature pages from actual annuity and brokerage account applications that were disguised as something else. Sometimes, they were told that actual accounts would be open, but that all profits would go to other terminally ill people. And they were always asked for personal information, like Social Security numbers, birthdates, driver's license numbers, etc.

Once armed with the fraudulently obtained identity information, Caramadre purchased annuities and death put bonds. And both he and Radhakrishnan took numerous steps to deceive the insurance companies and brokerage houses to hide Caramadre's true ownership interest.

Caramadre's scheme went on for about 15 years—from 1995 to 2010—until some of the insurance companies and brokerage houses he defrauded filed complaints and investigators with the FBI, U.S. Postal Inspection Service, Internal Revenue Service, and U.S. Attorney's Office began looking into the matter.

**Lesson to be learned.** If you or a family member is suffering, physically or financially, don't make quick business decisions...you still need to do your due diligence.

# Stopping a Would-Be Terrorist

## Who was One Chemical Away from Building a Bomb

The 20-year-old Saudi Arabian man living in Lubbock, Texas was intent on waging jihad against Americans—possibly even a former U.S. president—and he was one ingredient away from being able to build a powerful bomb.

**But Khalid Ali-M Aldawsari's deadly plans began to unravel when a shipping company's suspicions were raised—illustrating once again how the FBI relies on private industry and the general public in the fight against terror.**

In early February 2011, a Lubbock shipping firm received a package from a North Carolina chemical company containing 10 bottles of phenol intended for Aldawsari. Combined with just two other chemicals, phenol can be used to make a potent explosive. Delivering such poisonous chemicals to an individual's home is not common, so the shipping company contacted the North Carolina firm. Both decided that the phenol should not be delivered and that local law enforcement should be alerted. A Lubbock Police Department officer was called to the scene.

"That officer and his supervisor—because of their relationship with the FBI—decided that this was something we needed to know about," said Special Agent Frazier Thompson, who works in our Dallas Division. "Our initial focus was to identify Aldawsari to see if he had a legitimate reason for purchasing phenol."

In a matter of days, members of our North Texas Joint Terrorism Task Force learned that although Aldawsari had once been a chemical engineering student at Texas Tech, he was no longer enrolled there and had no affiliation with the university.

"He was trying to pass himself off as a Texas Tech student doing research on cleaning products," said Special Agent Mike Orndorff, who worked the investigation. "Those credentials, if legitimate, would have allowed him to buy the phenol."

Most alarming was that Aldawsari had already purchased the two other chemicals needed to make his bomb, along with test tubes, beakers, and protective gear. Through covert operations, investigators learned he had disassembled clocks and cell phones and stripped the wires off



Surveillance image of Khalid Ali-M Aldawsari

Christmas lights in apparent attempts to fashion timers and initiating devices.

**"His apartment bedroom was basically a storage room where he kept his chemicals and equipment," Thompson said. "He was sleeping in the living room on the couch or the floor."**

The investigation revealed troubling things about Aldawsari, who had come to the U.S. legally in 2008 on a student visa. "Based on evidence from the Internet and his journal entries," Thompson said, "Aldawsari was radicalized before he ever came to the United States. It appears he started planning this attack when he was a teenager and sought a scholarship to study specifically in America."

By this point, surveillance teams were monitoring Aldawsari around the clock. "He was searching online for large targets such as dams and electrical plants," Thompson said. He also searched for ways to conceal explosives in baby dolls and carriages and even sought the Texas address of former President George W. Bush.

On February 23, 2011, after agents were certain that Aldawsari was working alone, he was arrested and charged with attempted use of a weapon of mass destruction. In November, after being convicted by a jury, he was sentenced to life in prison.

"Aldawsari wanted to take out a lot of people," Thompson said. "It scares me to think what might have happened if we hadn't stopped him."



**Left: The 1998 arson at a Vail, Colorado ski resort caused more than \$24 million in damages.**

## Eco-Terrorist Surrenders

### Two Operation Backfire Fugitives Still at Large

After a decade as an international fugitive, Canadian citizen Rebecca Rubin gave up life on the run last week when she turned herself over to the FBI at the international border in Washington state.

**The 39-year-old alleged member of the domestic terrorist cell called “The Family” will face federal arson charges for her role in the largest eco-terrorism case in U.S. history, known as Operation Backfire. With Rubin in custody, only two members of The Family remain at large.**

Along with a dozen other conspirators, Rubin is charged with multiple crimes from 1996 through 2001 in the West and Pacific Northwest, including in Oregon, Colorado, and California. The Family committed an estimated \$48 million worth of arson and vandalism under the names of the Animal Liberation Front and the Earth Liberation Front.

The cell’s most notorious crime was the 1998 arson of a Vail, Colorado ski resort that caused more than \$24 million in damages and drew international attention to eco-terrorists—those who break the law in the misguided attempt to protect the environment and animal rights. The FBI took the lead in the Vail investigation, working closely with local, state, and federal law enforcement partners, and in 2004, multiple eco-terrorism investigations were condensed into Operation Backfire.

In July 2011, one of Rubin’s conspirators, Justin Solondz, was turned over to U.S. authorities by the Chinese government. Solondz had been imprisoned in China on drug

charges. That leaves two Operation Backfire fugitives still at large, and there is a reward for information leading to their arrest.

“Two years ago we had four fugitives. Now we have two—so we are halfway there,” said Special Agent Tim Suttles, who works in our Portland Division and has been investigating the eco-terrorist group since 2005.

Although Suttles said it is “very satisfying” to see Rubin surrender and submit herself to the judicial process, the Operation Backfire investigation will not be closed until the last two fugitives—Joseph Dibee and Josephine Overaker—are in custody.

**We need your help to locate these two individuals. A reward of up to \$50,000 each is being offered for information leading to the arrest of Dibee and Overaker, both of whom are believed to be living abroad.**

Here is what we know about the two:

- Dibee was indicted in 2006 on charges of arson, conspiracy, and animal enterprise terrorism. He was believed to be living in Syria with family members but may have fled the country due to the recent violence and upheaval there.



**Joseph Dibee and Josephine Overaker**

- Overaker was indicted in 2004 and 2006 for her involvement with the 1998 Vail arson and other crimes. She is believed to have spent time in Germany and may have settled in Spain. She speaks fluent Spanish.

**Suttles believes Rubin may have surrendered because she was tired of life on the run.** “She may have realized that being a fugitive meant she could never go home or could never have contact with her mom, who she is very close to.” Like many long-term fugitives, he added, “she may have come to the realization that coming in, admitting what you did, and taking your punishment will allow you to move on with your life.”

To date, Operation Backfire investigators have solved more than 40 criminal acts ranging from vandalism to arson. Seventeen individuals have been indicted, 15 of whom pled guilty and were sentenced in 2007 to jail time ranging from more than three years to 15 years.



# Hate Crimes Accounting

## Annual Report Released

In 2011, U.S. law enforcement agencies reported 6,222 hate crime incidents involving 7,254 offenses, according to our just-released *Hate Crime Statistics, 2011* report. These incidents included offenses like vandalism, intimidation, assault, rape, murder, etc.

The data contained in this report, which is a subset of the information that law enforcement submits to the FBI's Uniform Crime Reporting (UCR) program, includes the following categories: offense type, location, bias motivation, victim type, number of individual victims, number of offenders, and race of offenders.

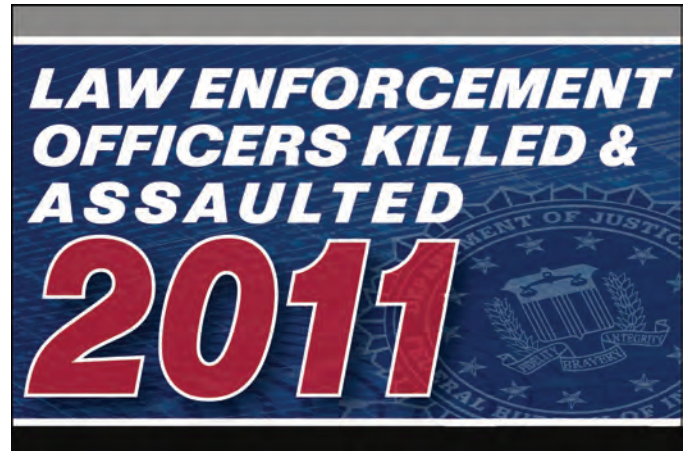
### Highlights from the 2011 Report:

- Of the 6,222 reported hate crimes, 6,216 were single-bias incidents—46.9 percent were racially motivated, 20.8 percent resulted from sexual orientation bias, 19.8 percent were motivated by religious bias, 11.6 stemmed from ethnicity/national origin bias, and 0.9 percent were prompted by disability bias.
- Law enforcement agencies reported 7,713 victims of hate crime—victims can be individuals, businesses, institutions, or society as whole. Sixty percent of these 7,713 were victims of crimes against persons, while 39.8 were victims of crimes against property.
- Thirty-two percent of the 6,222 hate crime incidents reported took place in or near residences; 18 percent took place on highways, roads, and alleys; and 9.3 percent took place at schools or colleges. The remaining percentage took place at locations like houses of worship, parking lots, bars, government and office buildings, etc.

### New in Hate Crime Reporting

Beginning in 2013, law enforcement agencies reporting hate crimes will be able to get even more specific when reporting bias motivation.

For example, the new bias categories of gender and gender identity—which added four new bias types—were added to the FBI's hate crime data collection as a result of the Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act. Other bias types were modified to comply with the race and ethnicity designations specified by the U.S. Office of Management and Budget. Data submitted under these new specifications will be part of the



UCR program's new system, scheduled to go online in the coming months. (The 2013 crime data will be published in 2014).

### FBI's Role in Investigating Hate Crimes

Hate crimes continue to be the highest priority of the Bureau's civil rights program because of their heinous nature and their impact on victims and communities. We investigate hate crimes that fall under federal jurisdiction, assist state and local authorities during their own investigations, and in some cases—with the U.S. Department of Justice Civil Rights Division—monitor developing situations to determine if federal action is appropriate.

In addition to responding to hate crimes, we're also taking a proactive approach to hate crimes overall. We're integrating a cadre of analysts with our experienced investigators to not only establish a national threat picture but to identify risk factors that can be used by FBI field offices to assess the potential for hate crimes at the local level.

### Increasing Hate Crime Awareness

Most of all, we're working to increase awareness of these crimes by establishing liaisons with civic and religious leaders and credible community organizations. Through our UCR program, we offer training to help law enforcement recognize hate crimes and also assist our partners in developing their own hate crimes training programs.



**Left:** Multiple long guns were seized in the case of Daniel Patrick Boyd, who conspired to kill Americans at home and abroad. He was sentenced in August to 18 years in prison.

## Homegrown Violent Extremism

### Dismantling the Triangle Terror Group

To his sons and others in their rural North Carolina community, Daniel Patrick Boyd was a charismatic figure. But the U.S. citizen used his persuasive powers to no good end—he promoted violent jihad against Americans at home and abroad.

**After a four-year investigation by the Raleigh-Durham Joint Terrorism Task Force (JTTF), Boyd and two of his sons, along with five other conspirators—known as the Triangle Terror Group—were arrested and charged with providing material support to terrorists and conspiring to murder persons overseas, including U.S. military personnel. Boyd pled guilty and was sentenced in August 2012 to 18 years in prison.**

Chris Briese, then-special agent in charge of our Charlotte office, noted at the time, “People who are plotting to harm Americans are no longer a world away from us.” The men and women of the JTTF who investigated the Boyd case learned that fact firsthand as they worked to unravel the network of homegrown violent extremists.

The case began in 2005 with a tip from someone in the Muslim community that one of its members was becoming radicalized. Boyd was a hero to young Muslim-Americans because at the age of 19 he had traveled to Pakistan and Afghanistan to receive military training and to fight with the mujahedeen.

In 2006, one of Boyd’s North Carolina jihad recruits traveled to Jordan and e-mailed his mentor to ask how

to get to the front lines to fight. “That’s when we began to understand how serious this threat was,” said Special Agent Paul Minella, a JTTF member who worked the case.

Over the next three years, the JTTF monitored the group—with the help of partner agencies and the support of the U.S. Attorney’s Office—using a variety of investigative tools, including court-ordered wiretaps and sources who infiltrated the group.

During one monitored conversation inside the food market Boyd owned, said Maria Jocys, who supervises the Raleigh-Durham JTTF, “in an effort to ingratiate himself with Boyd, one of the foreign-born co-conspirators bragged about his experience as a skilled sniper and graphically described how he shot a man overseas.”

**“The talk at the market was often about fighting jihad and how, in their belief, fighting jihad was an obligation,” added Special Agent Bill Logallo, another JTTF member.**

Investigators tracked Boyd’s network across the United States and six foreign countries. “It became very clear,” Jocys said, “that Boyd’s followers wanted to fight on the front lines overseas. And if they didn’t have the opportunity to do that, then they would wage jihad here at home.”

As the investigation continued, “we saw them buying a lot of weapons and ammunition,” Logallo said. Boyd dug a hole in his yard to bury a cache of weapons and positioned long guns in every room of his house. He took his sons and recruits out to train with weapons and taught them military tactics.

Even after Boyd suspected that the FBI was onto his group, “they kept going,” Minella said. “That’s how committed they were to jihad and how right they thought they were about their obligation to kill non-Muslims.”

After a carefully orchestrated takedown planned months in advance, Boyd and the rest of his Triangle Terror Group were arrested in July 2009. They had committed no acts of violence, but the JTTF was certain it was only a matter of time before they did.

“Boyd and his followers wanted to kill people,” Jocys said. “We had to stop them.”

# Help Catch Bank Robbers

## New Website Targets Suspects Nationwide

Bank robbers last year walked away from federally insured banks, credit unions, savings and loan associations, and armored trucks with more than \$38 million in cash, according to the last full year of FBI bank crime statistics. In one in five cases, the money was recovered. In the unsolved cases, surveillance images of suspects were often posted online—on FBI wanted posters and elsewhere—to enlist the public's help.

**To further that effort, the FBI has launched a new Wanted Bank Robbers website at [bankrobbers.fbi.gov](http://bankrobbers.fbi.gov), the first national system of its kind.**

The new site features a gallery of unknown suspects and a map function that plots robbery locations. Users can search by name, location, or other factors. Search results deliver a Wanted by the FBI poster that contains more images, a suspect's full description, and a brief narrative of the crime.

"This website is an operational tool that will help law enforcement identify and prosecute bank robbers more quickly, with the public's help," says Jason DiJoseph, who runs the bank robbery program at FBI Headquarters. "The idea is to make it easier for the public to recognize and turn in potential suspects and to draw connections between robberies in different cities and states."

**The FBI has had a primary role in bank robbery investigations since the 1930s**, when John Dillinger and his gang were robbing banks and capturing the public's imagination. In 1934, it became a federal crime to rob any national bank or state member bank of the Federal Reserve System. The law soon expanded to include bank burglary, larceny, and similar crimes, with jurisdiction delegated to the FBI. Today, the Bureau works with local law enforcement in bank robbery investigations, but the focus is mostly on violent or serial cases.

"Bank robbery sounds like an old-fashioned crime, but it is a dangerous and often violent criminal act that still results in the loss of lives and takes a significant toll on local communities," says DiJoseph.



**Bankrobbers.fbi.gov features a gallery of suspects and a fully integrated map feature; due to the sensitive nature of these crimes, robbers will not always appear on the map if the location is not publicized.**

Users of the new website can filter searches of serial and non-serial bank robbers. Following are some examples of serial cases:

- The AK-47 Bandit is sought in California, Idaho, and Washington for multiple bank robberies. The suspect often wears tactical gear and is armed with an AK-47-style assault rifle.
- A white male, aged 30-40, is wanted in Washington in connection with five armed bank robberies in the Seattle area since September.
- Two black males, believed to be in their 20s, are wanted in Virginia in connection with four armed bank robberies in March and April.

The bank crime statistics bear out the Bureau's emphasis on violent cases. While demand notes are bank robbers' most frequently used tools (2,958 times in 2011), they are followed by firearms (1,242 times) and the mere threat of weapons (2,331 times) or explosive devices (154 times). Even in cases where weapons have not been used, DiJoseph said, the risk of violence increases each time a serial bank robber strikes.

Of the 5,086 bank robberies, burglaries, and larcenies last year, 201 included acts of violence; 70 involved the discharge of firearms. Thirteen people were killed during bank robberies last year, though it was usually the perpetrator (10 incidents).

Visit the website to help us solve the most pressing bank robbery cases from our 56 field offices.





## Bank Fraud Hits Home

### Historic Community Credit Union Collapses

For years, the St. Paul Croatian Federal Credit Union in Eastlake, Ohio—about 30 miles northeast of Cleveland—had provided financial support to Croatians who had settled in the area and to others in the community. Through loans and additional services, the credit union helped many achieve their dreams of owning a home or business.

That all came to an end in April 2010, when the institution was placed into conservatorship and declared insolvent by the National Credit Union Administration—the independent federal body that oversees federal credit unions.

**The failure of the St. Paul Croatian Federal Credit Union, or SPCFCU, was one of the largest credit union collapses in American history, but it didn't have to happen.** Much of the blame has been placed squarely on the shoulders of its chief operating officer, Anthony Raguz, who over a 10-year period accepted more than \$1 million worth of bribes, kickbacks, and gifts in exchange for issuing a thousand fraudulent loans valued at more than \$70 million. Last month, Raguz was sentenced to 14 years in prison on charges of bank fraud, money laundering, and bank bribery and was ordered to pay \$71.5 million in restitution.

The fraudulent loans Raguz approved went to conspiring account holders who submitted paperwork listing minimal or no assets, income, or employment history. He also knowingly allowed borrowers to obtain loans using nominee names (family members, friends, business associates, etc.).

**After the loans were issued, most borrowers made little effort to pay them back.** To prevent these loans from appearing as delinquent on the books, Raguz directed the credit union to issue so-called reset loans (new loans made to cover delinquent payments on old loans) in the names of other SPCFCU members with active or even inactive accounts, deceased SPCFCU members, and fictitious businesses. Raguz even let some of the borrowers of the original fraudulent loans obtain additional loans.

**The crooked borrowers didn't get off scot-free:** so far, 16 have been convicted on various fraud charges. Some of the more prolific individuals include:

- Koljo Nikolovski, of Eastlake and Skopje, Macedonia, who fraudulently obtained several loans totaling more than \$5 million...none of which he paid back. He also wired \$2.3 million overseas to a bank account in Skopje. (At one point, he threatened Raguz if he refused to provide a loan or told anyone about previous loans.)
- Eddy Zai, an Eastlake businessman and the single largest recipient of fraudulent loans, who submitted false documents to defraud the credit union of approximately \$16.7 million.
- Arben Alia, of Eastlake, who fraudulently obtained several loans totaling approximately \$4.5 million, which he used—in part—to fund gambling excursions and to buy a bar.

**The impact of the credit union failure was significant:** Because the credit union was federally insured, innocent investors with accounts of \$250,000 or less were fully reimbursed. But some members with more money in their accounts—including some businesses and other institutions—were not reimbursed beyond that amount and ended up losing hard-earned dollars. And aside from the financial losses, the community lost an invaluable resource that had helped so many for so long.

Special thanks to the Cleveland office of the Internal Revenue Service-Criminal Investigation Division and the Eastlake Police Department for working this case with our Cleveland Field Office.

# A Byte Out of History

## The Hunt for Roger 'The Terrible' Touhy and His Gang

The careful plans were laid. In the early morning hours of December 29, 1942—70 years ago this month—FBI agents surrounded an apartment building on Kenmore Avenue in Chicago filled with a dangerous band of escaped convicts. With searchlights illuminating the building and nearby neighbors evacuated, an agent with a loudspeaker called for the men to surrender. Even Director J. Edgar Hoover was on hand.

**At the time, America was at war—fighting in theaters in Europe and the Far East during World War II.** The FBI was supporting the effort in many ways, protecting the homeland from espionage and sabotage and supplying valuable intelligence to its partners and to national leaders. One of its other wartime responsibilities was enforcing a newly enhanced Selective Service Act, which subjected all men of certain ages to either enter or register for military service. As it turns out, this law was the legal hook enabling the FBI to hunt down these criminals.

The prison break had taken place nearly three months earlier, on October 9. A group that included Roger "The Terrible" Touhy, Basil "The Owl" Banghart, Edward Darlak, and several other violent criminals escaped from the Stateville Penitentiary at Joliet, Illinois. They had guns smuggled in, cased the prison from all angles, and executed a well-planned break out.

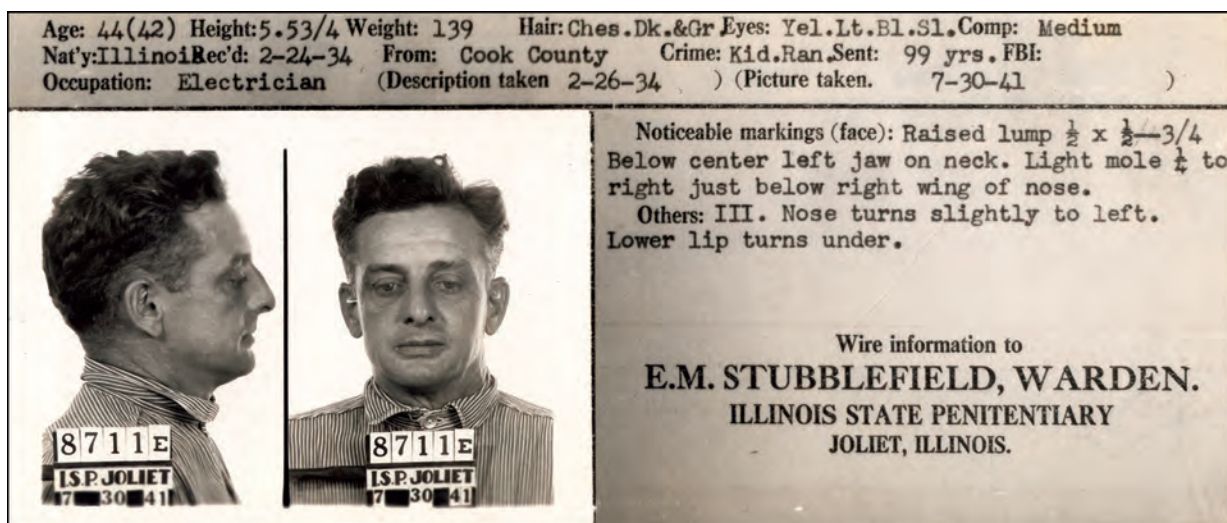
Stealing a guard's car, they sped away. Hours later, they abandoned the car openly in the middle of a small suburb

east of Chicago. It was their signal to the FBI that they didn't want to take the car across state lines and trigger Bureau jurisdiction. But they didn't realize that they would soon run afoul of the Selective Service Act. On October 16, one week after the no longer imprisoned criminals failed to register for the draft, the FBI entered the case.

**The FBI had numerous leads to begin its search for Touhy and his gang.** The Bureau knew Touhy well, arresting him nine years earlier on suspicion of being involved in the kidnapping of the president of a Minnesota brewing company. While in custody, Illinois courts convicted Touhy of abducting a rival criminal named John "Jake the Barber" Factor. Touhy was sent to prison in 1934.

Life on the run was not easy, and the gang began to have problems. Two members disobeyed the gang's rules and were nearly beaten to death. The gang moved often and was careful to cover its tracks. The Bureau figured that Touhy and his cohorts would use IDs stolen through pickpockets and muggings and worked with local police to collate these crimes and look for those assuming victims' identities.

**It worked, leading to the capture of the first fugitive.** More success followed. On December 16, agents observed a known acquaintance of one gang member participating in a suspicious meeting with an unknown contact. Agents tracked the unknown man, which led them to two more gang members (who died in a gunfight with Bureau agents) and ultimately to Touhy, Banghart, and Darlak. Following the early morning arrest, the gang was quickly returned to prison. They were home for the holidays—well, back in the big house anyway.



Roger "The Terrible" Touhy (above) and other violent criminals escaped from a penitentiary in Illinois in 1942.



## The Year in Review

### A Look at FBI Cases, Part 1

The FBI worked thousands of investigations during 2012 involving everything from terror plots to cyber theft, financial fraud, and crimes against children. As the year comes to a close, we take our annual look back at some of the Bureau's most significant cases.

**Part 1 focuses on our top investigative priority**—protecting the nation from terrorist attack. Working with local, state, federal, and international partners, we thwarted a number of potential attacks on U.S. citizens at home and abroad.

**Here are some of the top terror cases of 2012 in reverse chronological order:**

**Alabama men arrested on terrorism charges:** Two U.S. citizens living in Alabama were arrested in December and charged with planning to travel overseas to wage violent jihad. The pair met online and later confided their plans to an individual who—unbeknownst to them—was a confidential source working for the FBI.

**Plot to destroy Ohio bridge:** Four men were sentenced to prison in November for their roles in a conspiracy to destroy a bridge near Cleveland. The men—all self-proclaimed anarchists—pled guilty to conspiracy to use weapons of mass destruction. The group allegedly planned a series of crimes in the Cleveland area.

**Conspiracy to provide support to terrorists:** Four men were charged in Los Angeles in November with conspiring to provide material support to terrorists after they allegedly made arrangements to join al Qaeda and the Taliban in Afghanistan to kill Americans, among others.

**Plot to attack Pentagon and U.S. Capitol:** Also in November, a 27-year-old man was sentenced in Boston to 17 years in prison for plotting an attack on American soil and attempting to provide detonation devices to terrorists. The man built detonators for improvised explosive devices and provided them to FBI undercover operatives he believed were members of al Qaeda.

**Attempted bombing of New York Federal Reserve Bank:** A 21-year-old Bangladeshi national was arrested in October for attempting to detonate a 1,000-pound bomb in Lower Manhattan to strike the U.S. financial system on behalf of al Qaeda. The man allegedly traveled to the U.S. in January 2012 specifically to conduct a terrorist attack.

**Plot to attack U.S. Capitol:** A 29-year-old Virginia resident was sentenced to 30 years in prison in September for attempting to carry out a suicide bomb attack at the U.S. Capitol in February 2012.

**Plan to send weapons to Iraqi insurgents:** A former resident of Iraq residing in Kentucky pled guilty to terrorism charges in August for attempting to send Stinger missiles and other weapons to Iraq to be used against U.S. soldiers.

**'Revolution' leader sentenced:** A New York City resident was sentenced in June to more than 11 years in prison for using his position as a leader of the Revolution Muslim organization to promote violent extremism online against those he believed to be enemies of Islam.

**Violent extremists in Alaska:** Also in June, the leader of an Alaska militia was found guilty of conspiring to murder federal officials and possessing illegal firearms including silencers and grenade launchers.

**Supporting terrorism:** A 45-year-old Philadelphia resident was arrested in March and charged with conspiracy to provide material support to the Islamic Jihad Union, an extremist organization responsible for bombings and attacks against coalition forces in Afghanistan.

*Part 2: Fraud, fugitives, espionage, and more (page 107)*



# 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 2012, from cyber crimes to economic espionage and multi-million-dollar fraud schemes. As the year draws to a close, we take a look back at some of 2012'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:**

**Insider trading:** Charges against seven investment professionals were announced in New York in January alleging an insider trading scheme that netted nearly \$62 million in illegal profits.

**California gang takedown:** A total of 119 defendants were charged in San Diego in January with federal racketeering conspiracy, drug trafficking violations, and federal firearm offenses in one of the largest single gang takedowns in FBI San Diego history. The target was the Mexican Mafia gang and its affiliates.

**Economic espionage:** In February, a federal grand jury in San Francisco charged five individuals and five companies with economic espionage and theft of trade secrets in connection with their roles in a long-running effort to obtain U.S. trade secrets for the benefit of companies controlled by the People's Republic of China.

**Cyber hackers charged:** Several hackers in the U.S. and abroad were charged in New York in March with cyber crimes affecting over a million victims. Four principal members of the hacking groups Anonymous and LulzSec were among those indicted; another key member previously pled guilty to similar charges.

**Anchorage man indicted for murder:** In April, Israel Keyes was charged with the kidnapping and murder of an Anchorage barista. Keyes is believed to have committed multiple kidnappings and murders across the country between 2001 and March 2012. In December, after Keyes committed suicide in jail, the FBI requested the public's help regarding his other victims.

**Financial fraudster receives 110-year sentence:** In June, Allen Stanford—the former chairman of Stanford International Bank—was sentenced in Houston to 110 years in prison for orchestrating a 20-year investment fraud scheme in which he misappropriated \$7 billion to finance his personal businesses.



**Nationwide sweep recovers child victims of prostitution:** The FBI and its partners announced the results of Operation Cross Country, a three-day law enforcement action in June in which 79 child victims of prostitution were recovered and more than 100 pimps were arrested.

**International cyber takedown:** Also in June, a two-year FBI undercover cyber operation culminated in the arrest of 24 individuals in eight countries. The investigation focused on “carding” crimes—offenses in which the Internet is used to steal victims’ credit card and bank account information—and was credited with protecting over 400,000 potential cyber crime victims and preventing over \$205 million in losses.

**Health care fraud:** In July, global health care company GlaxoSmithKline pled guilty to fraud allegations and failure to report safety data and agreed to pay \$3 billion in what officials called the largest health care fraud settlement in U.S. history.

**Russian military procurement network:** In October, 11 members of a Russian military procurement network operating in the United States and Russia, as well as a Texas-based export company and a Russia-based procurement firm, were indicted in New York and charged with illegally exporting high-tech microelectronics from the U.S. to Russian military and intelligence agencies.

---

## 2012: The FBI Story Index

### ART THEFT

New Top Ten Art Crime: Reward Offered for Stolen Renoir Painting, page 77

### CIVIL RIGHTS

MLK Parade Bomber: Horrific Hate Crime Prevented; Case Solved, page 4

Human Trafficking Prevention: Help Us Identify Potential Victims, page 6

Protecting Civil Rights: Part 1: Memphis Agent Seeks Justice for Victims, page 10

Protecting Civil Rights: Part 2: Closing a Memphis Murder Case, page 11

Domestic Threat: White Supremacy Extremism, page 43

Teen Prostitution: Gang Used Social Media Sites to Identify Potential Victims, page 76

Hate Crimes Accounting: Annual Report Released, page 101

### COUNTERTERRORISM

On Guard Against WMD: Inside the Biological Countermeasures Unit, Part 1, page 15

On Guard Against WMD: Inside the Biological Countermeasures Unit, Part 2, page 16

Help Us Bring Bob Levinson Home: \$1 Million Reward Offered for Missing Retired FBI Agent, page 19

Eco-Terrorist Sentenced: Help Us Find Remaining Operation Backfire Fugitives, page 23

Domestic Threat: White Supremacy Extremism, page 43

Inside the Denver JTTF: Part 1: Vigilance Against Terrorism, page 55

Inside the Denver JTTF: Part 2: Partners Help Cast a Wide Safety Net, page 58

'Play How You Practice': FBI's WMD Training Workshop Tests Massive Response, page 61

Inside the Denver JTTF: Part 3: WMD Coordinator Focuses on Preparedness, Partnerships, page 63

Genocide and War Crimes: New Webpage Designed to Raise Awareness, Solicit Information, page 70

Living a Lie: Identity Theft That Lasted Decades, page 81

Help Us Catch a Terrorist: U.S. Citizen Wanted for Supporting al Qaeda, page 82

North to Alaska: Part 2: An Explosive Situation in the Dead of Winter, page 86

North to Alaska: Part 3: A Domestic Terrorist with a Deadly Plan, page 92

Two Most Wanted Terrorists Named: Third Man Sought for Questioning, page 93

Stopping a Would-Be Terrorist: Who was One Chemical Away from Building a Bomb, page 99

Eco-Terrorist Surrenders: Two Operation Backfire Fugitives Still at Large, page 100

Homegrown Violent Extremism: Dismantling the Triangle Terror Group, page 102

The Year in Review: A Look at FBI Cases, Part 1, page 106

### CRIMES AGAINST CHILDREN

A Mother's Worst Nightmare: Fusion Center Key in Rescue of Abducted Infant, page 5

Cyber Alerts for Parents & Kids: Tip #2: Beware of 'Sextortion,' page 12

Operation Atlantic: Taking International Aim at Child Predators, page 18

New Top Ten Fugitive: Child Pornographer Added to the List, page 29

Child Forensic Interviewers: Part 1: Providing Critical Skills on Sensitive Investigations, page 32

Child Forensic Interviewers: Part 2: Training Our Law Enforcement Partners, page 33

Looking for Our Children: National Missing Children's Day 2012, page 44

Operation Cross Country: Nationwide Sweep Recovers Child Victims of Prostitution, page 53

---

## 2012: The FBI Story Index

Infant Abductions: A Violent Trend Emerges, page 74

Teen Prostitution: Gang Used Social Media Sites to Identify Potential Victims, page 76

Safe Online Surfing: New Cyber Safety Website for Teachers, Students, page 85

### CRIMINAL JUSTICE INFORMATION SERVICES

Police Week: FBI Honors Law Enforcement's Sacrifices, page 40

Crimes Rates are Down: According to 2011 Preliminary Report, page 49

30-Year-Old Murder Solved: Fingerprint Technology Played Key Role, page 75

Latest Crime Stats: Annual Crime in the U.S. Report Released, page 89

Making the Ultimate Sacrifice: Report on Law Enforcement Officer Deaths Released, page 95

### CYBER CRIMES

Malware Targets Bank Accounts: 'Gameover' Delivered via Phishing E-Mails, page 2

Cyber Alerts for Parents & Kids: Tip #2: Beware of 'Sextortion,' page 12

Looking for Love?: Beware of Online Dating Scams, page 13

Operation Atlantic: Taking International Aim at Child Predators, page 18

The Cyber Threat: Part 1: On the Front Lines with Shawn Henry, page 25

The Cyber Threat: Part 2: Shawn Henry on Partnerships, Challenges, page 26

New Internet Scam: 'Ransomware' Locks Computers, Demands Payment, page 66

Safe Online Surfing: New Cyber Safety Website for Teachers, Students, page 85

Cyber Security: Focusing on Hackers and Intrusions, page 88

### DIRECTOR/FBI LEADERSHIP

Help Us Bring Bob Levinson Home: \$1 Million Reward Offered for Missing Retired FBI Agent, page 19

Community Leaders Recognized: Their Actions Improve Lives, page 22

The Cyber Threat: Part 1: On the Front Lines with Shawn Henry, page 25

The Cyber Threat: Part 2: Shawn Henry on Partnerships, Challenges, page 26

Major Financial Crime: Using Intelligence and Partnerships to Fight Fraud Smarter, page 28

A Byte Out of History: The Alvin Karpis Capture, page 35

The Hoover Legacy, 40 Years After: Part 1: The End of an Era, page 36

Police Week: FBI Honors Law Enforcement's Sacrifices, page 40

Remembering Giovanni Falcone: Italian Judge Assassinated by the Mafia 20 Years Ago, page 42

The Hoover Legacy, 40 Years After: Part 2: His First Job and the FBI Files, page 54

The Hoover Legacy, 40 Years After: Part 3: Another Side of J. Edgar, page 62

The Hoover Legacy, 40 Years After: Part 4: The Evolution of U.S. Intelligence, page 68

The Hoover Legacy, 40 Years After: Part 5: A Day in the Life, page 79

### FIELD CASES

Closing a 'Crime Superstore': Not-So Garden Variety Fraud in the Garden State, page 3

MLK Parade Bomber: Horrific Hate Crime Prevented; Case Solved, page 4

A Mother's Worst Nightmare: Fusion Center Key in Rescue of Abducted Infant, page 5

Human Trafficking Prevention: Help Us Identify Potential Victims, page 6



---

## 2012: The FBI Story Index

- Cargo Theft: How a Memphis Task Force Combats a Costly Problem, page 8
- Protecting Civil Rights: Part 1: Memphis Agent Seeks Justice for Victims, page 10
- Protecting Civil Rights: Part 2: Closing a Memphis Murder Case, page 11
- Cyber Alerts for Parents & Kids: Tip #2: Beware of 'Sextortion,' page 12
- Trying to Sell That Timeshare?: Beware of Fraudsters, page 14
- Help Us Bring Bob Levinson Home: \$1 Million Reward Offered for Missing Retired FBI Agent, page 19
- New Top Ten Fugitive: Child Pornographer Added to the List, page 29
- 'Booster' Behind Bars: Professional Shoplifter Gets Prison Term, page 31
- New Top Ten Fugitive: Help Us Find Adam Mayes, page 38
- The Case of the Misbranded Drug: Leads to Massive Fine and Penalties, page 45
- Journey Through Indian Country: Part 1: Fighting Crime on Tribal Lands, page 46
- New Top Ten Fugitive: Help Us Find a Rapist and Murderer, page 47
- Journey Through Indian Country: Part 2: Making an Impact on the Reservation, page 48
- Help Us Catch a Killer: Unknown Offender Linked by DNA in Two Separate Cases, page 50
- Journey Through Indian Country: Part 3: Murder on the Zuni Reservation, page 51
- Journey Through Indian Country: Part 4: Teamwork Makes a Difficult Job Easier, page 52
- Operation Cross Country: Nationwide Sweep Recovers Child Victims of Prostitution, page 53
- Inside the Denver JTTF: Part 1: Vigilance Against Terrorism, page 55
- Journey Through Indian Country: Part 5: A Zero-Tolerance Approach, page 56
- If It's Too Good to Be True: Massive Ponzi Scheme Proves Age-Old Adage, page 57
- Inside the Denver JTTF: Part 2: Partners Help Cast a Wide Safety Net, page 58
- Journey Through Indian Country: Part 6: Gaining Invaluable Experience on the Reservation, page 60
- Inside the Denver JTTF: Part 3: WMD Coordinator Focuses on Preparedness, Partnerships, page 63
- A Sordid Scam: Two Receive Life Sentences for Preying on Aspiring Models, page 65
- Mortgage Fraud: 'House King' was a Royal Con Man, page 69
- A Byte Out of History: Murder and the Dixie Mafia, page 73
- Living a Lie: Identity Theft That Lasted Decades, page 81
- Help Us Catch a Terrorist: U.S. Citizen Wanted for Supporting al Qaeda, page 82
- North to Alaska: Part 1: Smallest FBI Office Takes on Big Job, page 84
- North to Alaska: Part 2: An Explosive Situation in the Dead of Winter, page 86
- Remembering Lou Peters: Selfless Actions Brought Down Mob Boss, page 87
- Operation Universal Money Fast: Putting the Brakes on Health Care Fraud, page 91
- North to Alaska: Part 3: A Domestic Terrorist with a Deadly Plan, page 92
- LCD Price Fixing Conspiracy: Taiwanese Company, Execs Sentenced, page 94
- North to Alaska: Part 4: The Shot That Pierced the Trans-Alaska Pipeline, page 96
- Preying on the Weak: Estate Planner Victimized Terminally Ill, page 98
- Stopping a Would-Be Terrorist: Who was One Chemical Away from Building a Bomb, page 99

---

## 2012: The FBI Story Index

Homegrown Violent Extremism: Dismantling the Triangle Terror Group, page 102

The Year in Review: A Look at FBI Cases, Part 1, page 106

The Year in Review: A Look at FBI Cases, Part 2, page 107

### FOREIGN COUNTERINTELLIGENCE

Economic Espionage: How to Spot a Possible Insider Threat, page 39

Counterintelligence Awareness: Teaching Industry How to Protect Trade Secrets and National Security, page 97

### GENERAL

Helping Victims of Crime: Therapy Dog Program a First for the Bureau, page 34

### HISTORY

A Byte Out of History: Closing in on the Barker/Karpis Gang, page 7

Investigating Financial Crime: A Retrospective, page 21

A Byte Out of History: The Alvin Karpis Capture, page 35

The Hoover Legacy, 40 Years After: Part 1: The End of an Era, page 36

Celebrating Women Special Agents: Part 1: May 12, 1972—A New Chapter is Opened, page 41

Remembering Giovanni Falcone: Italian Judge Assassinated by the Mafia 20 Years Ago, page 42

The Hoover Legacy, 40 Years After: Part 2: His First Job and the FBI Files, page 54

Celebrating Women Special Agents: Part 2: Two Women Blaze a Trail in 1972, page 59

The Hoover Legacy, 40 Years After: Part 3: Another Side of J. Edgar, page 62

Celebrating Women Special Agents: Part 3: Early Pioneers Tell Their Stories, page 64

The Hoover Legacy, 40 Years After: Part 4: The Evolution of U.S. Intelligence, page 68

Celebrating Women Special Agents: Part 4: Who Said It? Pop Culture's Take on Women Special Agents, page 71

Celebrating Women Special Agents: Part 5: A Diversity of Backgrounds and Experiences, page 72

A Byte Out of History: Murder and the Dixie Mafia, page 73

Celebrating Women Special Agents: Part 6: Working Undercover, page 78

The Hoover Legacy, 40 Years After: Part 5: A Day in the Life, page 79

Remembering Lou Peters: Selfless Actions Brought Down Mob Boss, page 87

Celebrating Women Special Agents: Part 7: Two Have Made the Ultimate Sacrifice, page 90

A Byte Out of History: The Hunt for Roger 'The Terrible' Touhy and His Gang, page 105

### INTELLIGENCE

Overcoming the Language Barrier: Translation Center at the Ready to Assist U.S. Intelligence, page 1

FBI Financial Intelligence Center: Getting Ahead of Crime, page 24

Economic Espionage: How to Spot a Possible Insider Threat, page 39

The Hoover Legacy, 40 Years After: Part 4: The Evolution of U.S. Intelligence, page 68

Counterintelligence Awareness: Teaching Industry How to Protect Trade Secrets and National Security, page 97

### INTERNATIONAL

Operation Atlantic: Taking International Aim at Child Predators, page 18

Help Us Bring Bob Levinson Home: \$1 Million Reward Offered for Missing Retired FBI Agent, page 19

---

## 2012: The FBI Story Index

Eco-Terrorist Sentenced: Help Us Find Remaining Operation Backfire Fugitives, page 23

Economic Espionage: How to Spot a Possible Insider Threat, page 39

Remembering Giovanni Falcone: Italian Judge Assassinated by the Mafia 20 Years Ago, page 42

Genocide and War Crimes: New Webpage Designed to Raise Awareness, Solicit Information, page 70

FBI National Academy: Celebrating a Milestone, page 80

Help Us Catch a Terrorist: U.S. Citizen Wanted for Supporting al Qaeda, page 82

Two Most Wanted Terrorists Named: Third Man Sought for Questioning, page 93

LCD Price Fixing Conspiracy: Taiwanese Company, Execs Sentenced, page 94

Eco-Terrorist Surrenders: Two Operation Backfire Fugitives Still at Large, page 100

### LINGUIST/TRANSLATION PROGRAM

Overcoming the Language Barrier: Translation Center at the Ready to Assist U.S. Intelligence, page 1

### MAJOR THEFTS/VIOLENT CRIME

A Mother's Worst Nightmare: Fusion Center Key in Rescue of Abducted Infant, page 5

Cargo Theft: How a Memphis Task Force Combats a Costly Problem, page 8

Looking for Love?: Beware of Online Dating Scams, page 13

'Booster' Behind Bars: Professional Shoplifter Gets Prison Term, page 31

New Top Ten Fugitive: Help Us Find Adam Mayes, page 38

Journey Through Indian Country: Part 1: Fighting Crime on Tribal Lands, page 46

New Top Ten Fugitive: Help Us Find a Rapist and Murderer, page 47

Journey Through Indian Country: Part 2: Making an Impact on the Reservation, page 48

Crimes Rates are Down: According to 2011 Preliminary Report, page 49

Help Us Catch a Killer: Unknown Offender Linked by DNA in Two Separate Cases, page 50

Journey Through Indian Country: Part 3: Murder on the Zuni Reservation, page 51

Journey Through Indian Country: Part 4: Teamwork Makes a Difficult Job Easier, page 52

Operation Cross Country: Nationwide Sweep Recovers Child Victims of Prostitution, page 53

Journey Through Indian Country: Part 5: A Zero-Tolerance Approach, page 56

Journey Through Indian Country: Part 6: Gaining Invaluable Experience on the Reservation, page 60

A Sordid Scam: Two Receive Life Sentences for Preying on Aspiring Models, page 65

Infant Abductions: A Violent Trend Emerges, page 74

30-Year-Old Murder Solved: Fingerprint Technology Played Key Role, page 75

New Top Ten Art Crime: Reward Offered for Stolen Renoir Painting, page 77

Latest Crime Stats: Annual Crime in the U.S. Report Released, page 89

Making the Ultimate Sacrifice: Report on Law Enforcement Officer Deaths Released, page 95

Hate Crimes Accounting: Annual Report Released, page 101

Help Catch Bank Robbers: New Website Targets Suspects Nationwide, page 103

### ORGANIZED CRIME/DRUGS

Closing a 'Crime Superstore': Not-So Garden Variety Fraud in the Garden State, page 3



---

## 2012: The FBI Story Index

Human Trafficking Prevention: Help Us Identify Potential Victims, page 6

A Byte Out of History: Closing in on the Barker/Karpis Gang, page 7

Cargo Theft: How a Memphis Task Force Combats a Costly Problem, page 8

Remembering Giovanni Falcone: Italian Judge Assassinated by the Mafia 20 Years Ago, page 42

Operation Cross Country: Nationwide Sweep Recovers Child Victims of Prostitution, page 53

Teen Prostitution: Gang Used Social Media Sites to Identify Potential Victims, page 76

Remembering Lou Peters: Selfless Actions Brought Down Mob Boss, page 87

### **PARTNERSHIPS**

Overcoming the Language Barrier: Translation Center at the Ready to Assist U.S. Intelligence, page 1

MLK Parade Bomber: Horrific Hate Crime Prevented; Case Solved, page 4

A Mother's Worst Nightmare: Fusion Center Key in Rescue of Abducted Infant, page 5

Cargo Theft: How a Memphis Task Force Combats a Costly Problem, page 8

Protecting Civil Rights: Part 1: Memphis Agent Seeks Justice for Victims, page 10

Protecting Civil Rights: Part 2: Closing a Memphis Murder Case, page 11

Trying to Sell That Timeshare?: Beware of Fraudsters, page 14

Operation Atlantic: Taking International Aim at Child Predators, page 18

Police Week: FBI Honors Law Enforcement's Sacrifices, page 40

Remembering Giovanni Falcone: Italian Judge Assassinated by the Mafia 20 Years Ago, page 42

Journey Through Indian Country: Part 1: Fighting Crime on Tribal Lands, page 46

Journey Through Indian Country: Part 2: Making an Impact on the Reservation, page 48

Crimes Rates are Down: According to 2011 Preliminary Report, page 49

Help Us Catch a Killer: Unknown Offender Linked by DNA in Two Separate Cases, page 50

Journey Through Indian Country: Part 3: Murder on the Zuni Reservation, page 51

Journey Through Indian Country: Part 4: Teamwork Makes a Difficult Job Easier, page 52

Operation Cross Country: Nationwide Sweep Recovers Child Victims of Prostitution, page 53

Inside the Denver JTTF: Part 1: Vigilance Against Terrorism, page 55

Journey Through Indian Country: Part 5: A Zero-Tolerance Approach, page 56

Inside the Denver JTTF: Part 2: Partners Help Cast a Wide Safety Net, page 58

Journey Through Indian Country: Part 6: Gaining Invaluable Experience on the Reservation, page 60

'Play How You Practice': FBI's WMD Training Workshop Tests Massive Response, page 61

Inside the Denver JTTF: Part 3: WMD Coordinator Focuses on Preparedness, Partnerships, page 63

Insider Trading: Proactive Enforcement Paying Off, page 67

Genocide and War Crimes: New Webpage Designed to Raise Awareness, Solicit Information, page 70

30-Year-Old Murder Solved: Fingerprint Technology Played Key Role, page 75

FBI National Academy: Celebrating a Milestone, page 80

Living a Lie: Identity Theft That Lasted Decades, page 81

Cyber Security: Focusing on Hackers and Intrusions, page 88

Latest Crime Stats: Annual Crime in the U.S. Report Released, page 89

---

## 2012: The FBI Story Index

North to Alaska: Part 3: A Domestic Terrorist with a Deadly Plan, page 92

Making the Ultimate Sacrifice: Report on Law Enforcement Officer Deaths Released, page 95

North to Alaska: Part 4: The Shot That Pierced the Trans-Alaska Pipeline, page 96

Counterintelligence Awareness: Teaching Industry How to Protect Trade Secrets and National Security, page 97

Preying on the Weak: Estate Planner Victimized Terminally Ill, page 98

Hate Crimes Accounting: Annual Report Released, page 101

Homegrown Violent Extremism: Dismantling the Triangle Terror Group, page 102

Help Catch Bank Robbers: New Website Targets Suspects Nationwide, page 103

Bank Fraud Hits Home: Historic Community Credit Union Collapses, page 104

### **PUBLIC/COMMUNITY OUTREACH**

Cyber Alerts for Parents & Kids: Tip #2: Beware of ‘Sextortion,’ page 12

Looking for Love?: Beware of Online Dating Scams, page 13

The State of Financial Crime: Our Latest Accounting, page 17

Community Leaders Recognized: Their Actions Improve Lives, page 22

The Grandparent Scam: Don’t Let It Happen to You, page 27

Safe Online Surfing: New Cyber Safety Website for Teachers, Students, page 25

Help Catch Bank Robbers: New Website Targets Suspects Nationwide, page 103

### **PUBLIC CORRUPTION**

A Byte Out of History: Murder and the Dixie Mafia, page 73

### **RECRUITING/DIVERSITY**

Overcoming the Language Barrier: Translation Center at the Ready to Assist U.S. Intelligence, page 1

FBI Forensic Accountants: Following the Money, page 20

Celebrating Women Special Agents: Part 1: May 12, 1972—A New Chapter is Opened, page 41

Celebrating Women Special Agents: Part 2: Two Women Blaze a Trail in 1972, page 59

Celebrating Women Special Agents: Part 3: Early Pioneers Tell Their Stories, page 64

Celebrating Women Special Agents: Part 4: Who Said It? Pop Culture’s Take on Women Special Agents, page 71

Celebrating Women Special Agents: Part 5: A Diversity of Backgrounds and Experiences, page 72

Celebrating Women Special Agents: Part 6: Working Undercover, page 78

Celebrating Women Special Agents: Part 7: Two Have Made the Ultimate Sacrifice, page 90

### **TRAINING**

Child Forensic Interviewers: Part 1: Providing Critical Skills on Sensitive Investigations, page 32

Child Forensic Interviewers: Part 2: Training Our Law Enforcement Partners, page 33

Celebrating Women Special Agents: Part 1: May 12, 1972—A New Chapter is Opened, page 41

Celebrating Women Special Agents: Part 2: Two Women Blaze a Trail in 1972, page 59

‘Play How You Practice’: FBI’s WMD Training Workshop Tests Massive Response, page 61

Celebrating Women Special Agents: Part 3: Early Pioneers Tell Their Stories, page 64

FBI National Academy: Celebrating a Milestone, page 80

Making the Ultimate Sacrifice: Report on Law Enforcement Officer Deaths Released, page 95

---

## 2012: The FBI Story Index

### WHITE-COLLAR CRIME

Closing a 'Crime Superstore': Not-So Garden Variety Fraud in the Garden State, page 3

Investigating Insurance Fraud: A \$30-Billion-a-Year Racket, page 9

Trying to Sell That Timeshare?: Beware of Fraudsters, page 14

The State of Financial Crime: Our Latest Accounting, page 17

FBI Forensic Accountants: Following the Money, page 20

Investigating Financial Crime: A Retrospective, page 21

FBI Financial Intelligence Center: Getting Ahead of Crime, page 24

The Grandparent Scam: Don't Let It Happen to You, page 27

Major Financial Crime: Using Intelligence and Partnerships to Fight Fraud Smarter, page 28

Bankruptcy Fraud: Creditors and Consumers Pay the Price, page 30

Nursing Home Abuse: Owner Cheats Government and Neglects Residents, page 37

The Case of the Misbranded Drug: Leads to Massive Fine and Penalties, page 45

If It's Too Good to Be True: Massive Ponzi Scheme Proves Age-Old Adage, page 57

Insider Trading: Proactive Enforcement Paying Off, page 67

Mortgage Fraud: 'House King' was a Royal Con Man, page 69

Living a Lie: Identity Theft That Lasted Decades, page 81

Distressed Homeowner Initiative: Don't Let Mortgage Fraud Happen to You, page 83

Operation Universal Money Fast: Putting the Brakes on Health Care Fraud, page 91

LCD Price Fixing Conspiracy: Taiwanese Company, Execs Sentenced, page 94

Counterintelligence Awareness: Teaching Industry How to Protect Trade Secrets and National Security, page 97

Preying on the Weak: Estate Planner Victimized Terminally Ill, page 98

Bank Fraud Hits Home: Historic Community Credit Union Collapses, page 104



**FBI OFFICE OF PUBLIC AFFAIRS**

935 Pennsylvania Avenue NW

Washington, D.C. 20535



Insulated in a full-blast suit, a bomb technician demonstrates equipment used to neutralize an improvised explosive device.