



# THE FBI STORY

2015







# THE FBI STORY

2015

[www.fbi.gov](http://www.fbi.gov)



During a training exercise, FBI medics prepare a wounded agent for helicopter transport to a hospital. Training scenarios are meant to mimic real-world conditions, which can include hostile environments accessible only by helicopter. See story on pages 64-65.



### A Message from FBI Director James B. Comey

For the FBI, 2015 was an incredible year. We, along with our partners, were at the center of the struggle for security in the face of terrorism, crime, and cyber attacks. Together we arrested corrupt public officials and white-collar criminals. We dismantled hacker networks and took down transnational syndicates at home and overseas. We disrupted human trafficking operations and stopped violent gangs from infiltrating our neighborhoods. And we protected Americans from an ever-evolving host of terrorist threats.

To get a sense of the challenges we faced and what we accomplished in 2015, here is the latest edition of *The FBI Story*. Our annual collection of news and feature articles from the Bureau's public website highlights some of our recent investigations and operations. These include the indictments of more than a dozen high-ranking officials of FIFA—the governing body of international soccer—for their roles in a decades-long bribery scheme and a nationwide child exploitation sweep that recovered 149 young victims. *The FBI Story* also tells how we helped dismantle a Detroit crime ring responsible for “smash and grab” jewelry store robberies in a half-dozen states and how we worked with our partners to take down an underground forum where hackers bought and sold malware, personal information, and software to facilitate cyber crimes across the globe.

This edition of *The FBI Story* also features some of the Bureau's unique capabilities. You will read about the Cyber Action Team, which can rapidly deploy just about anywhere in the world to quickly and expertly preserve evidence after a cyber intrusion. You will learn about how we helped create *The Company Man*, a film about the threat of economic espionage. And you will discover the importance of the National Incident-Based Reporting System, or NIBRS, which gives a fuller picture of the circumstances and context surrounding criminal activity. With better data, we are better prepared to fight crime and keep people safe, and we can better adapt to changing threats.

We know 2016 will be difficult. The threats we face are moving faster and becoming harder to anticipate and stop. As these stories illustrate, we don't face these challenges alone. We rely on strong partnerships with law enforcement, intelligence agencies, and the private sector. We need everyone to work together to keep us secure, both here at home and abroad.

Thank you for your support of the FBI. Everything we accomplish depends upon the American people believing us, trusting us, and seeing us for what we are—honest, competent, and independent. On behalf of the entire FBI, I hope you enjoy this latest edition of *The FBI Story*. We look forward to working for you and with you in 2016.

A handwritten signature in black ink that reads "James B. Comey". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.





FBI Director James Comey shares his thoughts on the relationship between law enforcement personnel and the diverse communities they serve and protect during a speech at Georgetown University in Washington, D.C. on February 12, 2015. See story on page 18.







# Adopt-A-School Program

## Part 1: Bringing a Message of Hope to Students



**Left: Junior Special Agents from Bucknell Elementary School in Alexandria, Virginia tour the U.S. Capitol.**

Twenty years ago, the FBI began a program to help kids steer clear of drugs and gangs while learning core values that would make them good citizens. Since the Adopt-A-School Program was established in 1994, special agents and other FBI employees have volunteered thousands of hours to make a positive impact on young people around the nation.

The Adopt-A-School Program identifies schools in disadvantaged communities—where kids may face greater exposure to gangs, drugs, and criminal activity—and sends Bureau employees there to be tutors and mentors.

“This is a great program that can have a profound influence on young people,” said Special Agent Paul Geiger, chief of the Community Relations Unit at FBI Headquarters in Washington. “We teach students that despite any hardships they may be facing now, if they work hard and make the right decisions, they can accomplish anything they want with their lives.”

The Adopt-A-School Program contains different components

aimed at specific age groups. The Junior Special Agent program, for example, is directed at fifth- and sixth-graders. A mentorship program is aimed at second- and fourth-graders, and the Future Agents in Training program is for high school students between the ages of 16 and 18. Depending on the component, Bureau employees may visit schools once a week for several months, or every other week for an entire school year.

“It’s all volunteer on the part of FBI employees,” Geiger explained, “and there is no cost to the taxpayer because funds needed for field trips and other items are typically raised through our Citizens Academy Alumni Associations.”

In the last fiscal year—October 1, 2013 to September 30, 2014—28 FBI field offices had active Adopt-A-School programs, and more than 800 students nationwide graduated from Junior Special Agent programs.

The Washington Field Office, located near FBI Headquarters, has one of the largest—and oldest—Adopt-A-School programs. This year, community outreach

specialists there are administering the program to six different schools in the region, and more than 300 young people are participating.

“We have a curriculum with core blocks of instruction that integrates with what the kids are learning in the classroom,” said Special Agent William Woodson. “Students also learn about what the men and women of the FBI do—from bomb techs and SWAT teams to evidence collectors and investigators.”

“We teach our Junior Special Agents about the dangers of gangs and drugs, about cyber-bullying, and how to stay safe online,” Woodson added. “We teach them core values like honesty, integrity, and responsibility.” Fitness is also an important part of the program, and before they graduate and become Junior Special Agents, students must pass a fit test.

During the school year, youngsters in the Washington Field Office program are taken on field trips to the White House, the U.S. Capitol, and nearby Civil War sites. “The trips are fun but also educational,” Woodson explained. “We are not going to an amusement park. We are doing things that are educational.”

He added that for many of the students, who come from difficult socioeconomic backgrounds, the field trips are a rare privilege. “Even though some of these kids live only a few miles from downtown Washington, they might never see the Capitol or the White House if not for this program.”



# Adopt-A-School Program

## Part 2: Becoming a Junior Special Agent

The 22 fifth-graders who participated in a Junior Special Agent Program last summer sponsored by the FBI's San Diego Field Division live in a tough neighborhood, and few of them have a permanent place to call home.

"We chose the Monarch School because it's in one of our high-crime areas," said Cheryl Dorenbush, a community outreach specialist in our San Diego Office who organized the program. "Every kid in the class was in some stage of homelessness. Most were in shelters or temporary housing, and some were living out of cars. This is where we thought we could have the biggest impact."

The Junior Special Agent Program—one component of the Bureau's Adopt-A-School Program—aims to give fifth- and sixth-graders in disadvantaged

neighborhoods the information, skills, and discipline they need to stay away from gangs, drugs, and crime. Along the way, students learn about the FBI and the ways in which law enforcement helps to serve and protect their communities.

One of the most important pieces of information the 10- and 11-year-old San Diego students received was simple but powerful: Where you start in life doesn't have to dictate where you end up. And one FBI employee who took part in the program drove that point home when she arrived in the classroom.

Special Agent Josie Regula grew up two blocks from the Monarch School in the Logan Heights section of San Diego. Her family was poor, and as a young girl, Regula saw that gang members seemed to have the most power and get the most respect in the

neighborhood. She told her mom she wanted to join a gang.

Speaking to the students in Spanish, Regula told her story: How, thanks to her mom, she didn't join a gang, and despite the odds, she eventually went to college and later joined the FBI (see sidebar on next page).

"A lot of kids' role models are older siblings, and those siblings can turn out to be gangsters and criminals and drug dealers," Regula said. "I tell the kids, 'You don't have to do that.' Many of these kids are never told they can be more than their older brother."

"My goal is to make sure they understand there is an option out there to move forward," she explained. "You can achieve great success, as long as you make good decisions and don't let people tell you what you can't do."



"A lot of these children don't have positive role models," she added. "The neighborhood they live in is a very rough area, heavily populated by gangs, with drugs and crime. Lots of parents are working two jobs and don't have time to be with their children. The kids need to hear this message."

During the 11-week program, FBI employees and members of other law enforcement organizations visited the students and taught them how to use their brains to avoid the dangers of drugs and gangs, to stay safe online, and to recover and analyze evidence from a crime scene. Students also learned about the FBI's core values, such as honesty and integrity.

"The agents were amazing," said teacher Kristin Dragomire. "They dove in and talked to the kids and answered all their questions. It wasn't like they were just coming

in and giving a lecture about their jobs."

She added, "Most of the students have a parent who is incarcerated, brothers and sisters who have been arrested. Many have experienced domestic violence where law enforcement has become involved. So they are used to seeing law enforcement in the context of traumatic situations. This was a very different and welcoming experience for the kids."

The students—some of whom had never exercised in an organized way before—also committed to an "Agent Boot Camp" three days a week that consisted of doing sit-ups, push-ups, and running. At the end of the program, after a tour of the FBI's San Diego headquarters, they were given a fitness test before receiving their Junior Special Agent badges and credentials.

"This was such a unique opportunity for kids who are so underserved and under-represented," Dragomire said. "It made a big impact on them."

"My favorite part was getting to meet all the agents—they looked like they were a family," said Quethzali Osuna, one of the fifth-graders in the program. "What I really like is how they were protecting us from all the dangerous stuff out there. They showed us and told us what they had to do—to exercise and stay healthy."

Another student, Josh Romero, said the program taught him that staying away from bad influences and making good decisions is key to becoming successful in life. "Don't mess up your future," he said.



#### **A Positive Role Model**

Special Agent Josie Regula grew up in a poor San Diego neighborhood rife with gangs, drugs, and crime. Her mother was a house cleaner and her father was a gardener. Her high school counselor's hope was that she would become a secretary.

"That would be a good career for you," she remembers being advised. "As a little kid, that's what I was told I could do."

She and her family had no money for college, and Regula didn't even entertain the idea of an education beyond high school. When she was growing up, "the only thing I saw was gangs. I wanted to be a gangster, because that's who got respect in the neighborhood. I didn't know any better."

Her mom, who only had a second-grade education, was smart enough to know that joining a gang was the wrong thing to do. "I want more for you," she told her daughter, and Regula listened.

After graduating from high school, she got a job at the U.S. Attorney's Office in downtown San Diego. When her mother heard the news, she was proud. "You are going to work inside an office, not cleaning an office," her mom said.

During three years there, she rose through the ranks from student clerk to typist and then receptionist. She later took a job with an attorney who encouraged her to go to college. She

enrolled, graduated with a teaching certificate, and planned on a career as a teacher.

By chance, though, she talked with an FBI agent at a job fair at San Diego State University, who encouraged her to consider a language specialist position in the Bureau. Regula, who speaks Spanish and English, took a language test, passed, and was offered the job.

Regula joined the Bureau in 1992 and was a language specialist for four years before becoming an agent. She has worked child prostitution cases, drug cases, civil rights violations, and human trafficking investigations and is now a senior polygrapher.

"I can't believe this is where I've gotten to," Regula said. She is happy to share her story with students from her old neighborhood. "When they see me walk in the room, speaking in their native tongue, and learn how I got to be an FBI agent, you can tell they appreciate the message that they can do this, too."



# Adopt-A-School Program

## Part 3: 'I Promise to be a Good Citizen'

The nearly 30 sixth-graders at Bucknell Elementary School in Alexandria, Virginia stood at their desks, raised their right hands, and recited in unison a pledge they knew well: "I accept the position of junior special agent of the Federal Bureau of Investigation. I promise to be a good citizen. I will obey all the laws of my country and do my best in school. I will make the right choices by remaining drug free, staying in school, and practicing non-violent behavior in handling difficult situations."

That pledge begins every session of the FBI's Junior Special Agent Program, which aims to give fifth- and sixth-graders in disadvantaged neighborhoods the skills and discipline they need to steer clear of gangs, drugs, and crime.

Located just outside the District of Columbia, Bucknell was one of the first schools to embrace the

FBI's Adopt-A-School outreach program 20 years ago. Now, the Washington Field Office administers the program to six schools in and around the nation's capital, dispatching agents and other Bureau employees throughout the school year to be tutors and mentors to more than 300 young people annually.

"During the past two decades we have reached thousands of kids," said Special Agent William Woodson. "Our goal is to provide opportunities for these young people who might not have had them otherwise."

The Junior Special Agent Program at Bucknell consists of core blocks of instruction that integrate with classroom curriculum. For example, when the students learn about the Civil War and the Emancipation Proclamation, they take field trips to battlefield sites and the

U.S. Capitol to reinforce what they learn. Funds for the trips are provided by the local Citizens Academy Alumni Association, a non-profit organization that supports the Adopt-A-School Program and uses no taxpayer money. The students also meet a variety of FBI agents who talk to them about gangs and drugs, as well as core values such as integrity, respect, and honesty. And the program requires students to exercise on a regular basis.

"We are helping to make sure that the kids don't do drugs and stay in school," Woodson said. "Our agents have a positive influence on them."

"The FBI is teaching our students to do the right thing and believe in themselves," said Paul Adams, who participated with the Junior Special Agent Program for nine years as a Bucknell teacher and now serves as a liaison between the school and



Special Agent William Woodson of the FBI's Washington Field Office leads a Junior Special Agents Program lesson about Internet safety for sixth-graders in Alexandria, Virginia.



the Washington Field Office. “This program shows our young people that no matter where you come from or what your background is, you can succeed.”

Sixth-grade teachers Nisreen Daoud and Amanda Frank are getting their first exposure to the Junior Special Agent Program this year at Bucknell. “A lot of our students go home to empty houses,”

Daoud explained. “Their parents are working all the time. This is their safe zone. They feel at home when they are at school.” And because the Junior Special Agent Program has been a fixture at Bucknell for so long, the students look forward to it. “They can’t wait until they get to sixth grade,” Daoud said. “The first day of school the kids were like, ‘When is the FBI program starting?’ ”

“One of our goals is to give these elementary students their first taste of the FBI,” said Woodson. “We want to groom young leaders.” He added, “This program teaches them core values that we hope they will carry into adulthood so they can become great community ambassadors in whatever they choose to do.”





# Armenian Criminal Enterprise Dealt Serious Blow

## Cooperative Law Enforcement Effort was Key

In May 2008, a massive shootout between Armenian Power and another California gang on the streets of North Hollywood ended with the deaths of two rival gang members. And while local law enforcement and the FBI already had Armenian Power on their radar, this deadly firefight on the streets of a major American city raised the group's profile—and resulted in efforts by the FBI and its partners to go after Armenian Power and its leadership through federal racketeering statutes.

The investigation revealed that this street gang was actually an international organized criminal enterprise whose illegal activities ranged from bank fraud and identity theft to violent extortion and kidnappings. It also revealed that this enterprise victimized its own Armenian community in California. By 2011, we had enough evidence to charge 90 Armenian Power leaders, members, and associates in two separate indictments.

Of those 90 charged, 87 have been convicted, including one of the enterprise's primary leaders—Mher Darbinyan—who was recently sentenced to 32 years in prison. (Of the three remaining indicted individuals, prosecutors dropped the charges against one, and the other two are currently fugitives.)

According to Agent Jeremy Stebbins, who worked the case out of our Los Angeles Office, “With the arrests and convictions of nearly all senior leadership of Armenian Power, we dealt a serious blow to their ability to continue to operate in the manner they were accustomed. We also sent a message to the Eurasian organized crime community that they are being targeted and watched.”

Armenian Power leadership was based in California, but the group's operations—particularly its fraud schemes—involved the use of phony businesses located in cities throughout the United States. And Armenian Power leaders had dealings with organized crime figures in places like Armenia and Russia.

### Potentially Dangerous Leak Uncovered During Case

During the multi-agency investigation into the Armenian Power criminal enterprise, we were also able to identify the source of an information leak within the federal district court clerk's office in Los Angeles. A clerk's office employee and her husband were charged and later convicted for their roles in a scheme to access and disclose information contained in sealed court documents to tip off organized crime figures and gang members prior to their arrests. Some of those compromised records concerned individuals who were members or associates of the Armenian Power criminal enterprise and subjects of pending federal arrest warrants.

This kind of criminal activity often threatens the safety of law enforcement agents and officers—particularly during large-scale takedowns of violent criminal enterprises and their members.

Law enforcement was also able to uncover ties between Armenian Power and the Mexican Mafia, the prison gang that controls much of the narcotics distribution and other criminal activity within California's correctional facilities. The Mexican Mafia would protect Armenian Power members and associates who were behind bars, while Armenian Power members and associates on the outside would help facilitate Mexican Mafia criminal activities.

During the course of the investigation, we rescued a kidnapped victim and were able to



Shown here are some of the firearms seized during a multi-agency investigation into the activities of the California-based Armenian Power criminal enterprise.

charge several additional subjects with kidnapping, extortion, and other violent crimes. We also seized more than \$3 million in fraudulently obtained luxury automobiles. And we interfered in several violent confrontations between rival groups, arresting more gang members and seizing firearms.

Court-authorized wiretaps on 25 different phone numbers were a key part of the case. Through these conversations, we were able to obtain a wealth of incriminating evidence as defendants spoke about targeting wealthy Armenians for robbery, planning check fraud activity, making illegal firearms deals, installing skimmers on ATMs, watering illegal marijuana plants in a warehouse, mailing illegal narcotics to customers, planning kidnappings, and extorting money from victims using threats of violence.

This complicated and multi-subject case was investigated by the Eurasian Organized Crime Task Force, led by the Bureau's Los Angeles Division and the Glendale Police Department. Other vital task force members include several local California police and sheriff's departments and a number of federal agencies.

# Extreme Case of Witness Intimidation

## Justice for Six Slain Victims in Philadelphia



**Left:** This Philadelphia row house was firebombed by individuals who worked for Philadelphia drug trafficker Kaboni Savage. Four children and two adults, family members of a federal witness, died in the fire. The adjacent row homes were also damaged.

As far as witness intimidation goes, Philadelphia drug trafficker Kaboni Savage and members of his criminal enterprise appeared to corner the market on how far they'd go to silence anyone willing to testify against the organization. The most horrifying example of this was the brutal firebombing that resulted in the deaths of six members of a federal witness' family in retaliation for his cooperation with law enforcement.

But a long-term, multi-agency investigation eventually proved that Kaboni Savage was responsible for those six murders—and at least six others—and that he headed a drug trafficking enterprise that excelled in using violence and other criminal tactics against anyone who threatened its drug trade. Recently, the final defendant charged in the firebombing deaths was sentenced to 40 years in prison, and Savage himself, convicted in 2013 on murder and racketeering charges, eventually received the death sentence.

In the late 1990s, Kaboni—then a small-time drug dealer—began buying cocaine in bulk and building his criminal organization. He was making a name for himself, especially for his often-brutal methods of operation—which included murders, beatings, kidnappings, and threats—

against anyone who crossed him (customers, rival gang members, his own underlings, even law enforcement).

Law enforcement, however, had Kaboni in their cross hairs, and he and his organization soon became the focus of an investigation by the Philadelphia FBI's Safe Streets Task Force, made up of local, state, and federal agencies. In May 2004, Kaboni and others were indicted for conspiring to distribute cocaine, money laundering, firearms offenses, and later on, witness intimidation. The perpetrators were arrested and held for trial.

It was from jail that Savage orchestrated the arson murder of six members of Eugene Coleman's family. Coleman, a member of Savage's gang who was among those named in the May 2004 indictment, had agreed to cooperate in the case. Through visits with family members—including his sister, Kidada—and surreptitious phone calls with other gang members, Savage planned the murders and solicited the help of his sister and two other gang members—Lamont Lewis and Robert Merritt. Kidada Savage passed the plan on to the other two and identified the Coleman home. Then Lewis and Merritt, in the early morning hours of October 9, 2004, drove to the Philadelphia

row house, fired warning shots into the residence, and threw two full gasoline cans with a lit cloth fuse into the home.

After extinguishing the flames, the fire department found the bodies of six victims—Coleman's 54-year-old mother, his 15-month-old son, and four other relatives, including a 10-year-old girl and 12- and 15-year-old boys. (Coleman was incarcerated at the time of the arson.) Through investigative techniques like court-authorized electronic surveillance and the use of informants, members of the task force were eventually able to collect evidence—some of it in Kaboni Savage's own words—of how the plot was hatched and carried out.

Kaboni Savage and four of his associates went to trial in November 2004 on the initial drug trafficking charges—14 others had already pled guilty before trial—and were convicted and sentenced. Eventually, though, Kaboni Savage and a number of his associates—including Kidada Savage—were indicted and ultimately convicted by a federal grand jury looking into the arson deaths of Coleman's family.

By the time it was all over, Kaboni Savage's criminal organization was dismantled—thanks in part to former associates and others willing to testify against him. And those six innocent people murdered in their home—one of many ruthless attempts by Savage to keep his operations running—finally received justice.



# Ransomware on the Rise

## FBI and Partners Working to Combat This Cyber Threat

Your computer screen freezes with a pop-up message—supposedly from the FBI or another federal agency—saying that because you violated some sort of federal law your computer will remain locked until you pay a fine. Or you get a pop-up message telling you that your personal files have been encrypted and you have to pay to get the key needed decrypt them.

These scenarios are examples of ransomware scams, which involve a type of malware that infects computers and restricts users' access to their files or threatens the permanent destruction of their information unless a ransom—anywhere from hundreds to thousands of dollars—is paid.

**Ransomware doesn't just impact home computers.** Businesses, financial institutions, government agencies, academic institutions, and other organizations can and have become infected with it as well, resulting in the loss of sensitive or proprietary information, a disruption to regular operations, financial losses incurred to restore systems and files, and/or

potential harm to an organization's reputation.

Ransomware has been around for several years, but there's been a definite uptick lately in its use by cyber criminals. And the FBI, along with public and private sector partners, is targeting these offenders and their scams.

**When ransomware first hit the scene, computers predominately became infected with it when users opened e-mail attachments that contained the malware.**

But more recently, we're seeing an increasing number of incidents involving so-called "drive-by" ransomware, where users can infect their computers simply by clicking on a compromised website, often lured there by a deceptive e-mail or pop-up window.

Another new trend involves the ransom payment method. While some of the earlier ransomware scams involved having victims pay "ransom" with pre-paid cards, victims are now increasingly asked to pay with Bitcoin, a decentralized virtual currency network that

attracts criminals because of the anonymity the system offers.

Also a growing problem is ransomware that locks down mobile phones and demands payments to unlock them.

### Latest Ransomware Threat

A fairly new ransomware variant has been making the rounds lately. Called CryptoWall (and CryptoWall 2.0, its newer version), this virus encrypts files on a computer's hard drive and any external or shared drives to which the computer has access. It directs the user to a personalized victim ransom page that contains the initial ransom amount (anywhere from \$200 to \$5,000), detailed instructions about how to purchase Bitcoins, and typically a countdown clock to notify victims how much time they have before the ransom doubles. Victims are infected with CryptoWall by clicking on links in malicious e-mails that appear to be from legitimate businesses and through compromised advertisements on popular websites. According to the U.S. CERT, these infections can be devastating and recovery can be a difficult process that may require the services of a reputable data recovery specialist.

For more information on ransomware in general, visit the U.S. CERT website at [www.us-cert.gov](http://www.us-cert.gov).





The FBI and our federal, international, and private sector partners have taken proactive steps to neutralize some of the more significant ransomware scams through law enforcement actions against major botnets that facilitated the distribution and operation of ransomware.

For example:

- Reveton ransomware, delivered by malware known as Citadel, falsely warned victims that their computers had been identified by the FBI or Department of Justice as being associated with child pornography websites or other illegal online activity. In June 2013, Microsoft, the FBI, and our financial partners disrupted a massive criminal botnet built on the Citadel malware, putting the brakes on Reveton's distribution.
- Cryptolocker was a highly sophisticated ransomware that used cryptographic key pairs to encrypt the computer files of its victims and demanded ransom for the encryption key. In June 2014, the FBI announced—in conjunction with the Gameover

Zeus botnet disruption—that U.S. and foreign law enforcement officials had seized Cryptolocker command and control servers. The investigation into the criminals behind Cryptolocker continues, but the malware is unable to encrypt any additional computers.

If you think you've been a victim of Cryptolocker, visit the Department of Homeland Security's U.S. Computer Emergency Readiness Team (CERT) CryptoLocker webpage for remediation information.

The FBI—along with its federal, international, and private sector partners—will continue to combat ransomware and other cyber threats. If you believe you've been the victim of a ransomware scheme or other cyber fraud activity, please report it to the Bureau's Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov).

### Protect Your Computer from Ransomware

- Make sure you have updated antivirus software on your computer.
- Enable automated patches for your operating system and web browser.
- Have strong passwords, and don't use the same passwords for everything.
- Use a pop-up blocker.
- Only download software—especially free software—from sites you know and trust (malware can also come in downloadable games, file-sharing programs, and customized toolbars).
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if you think it looks safe. Instead, close out the e-mail and go to the organization's website directly.
- Use the same precautions on your mobile phone as you would on your computer when using the Internet.
- To prevent the loss of essential files due to a ransomware infection, it's recommended that individuals and businesses always conduct regular system back-ups and store the backed-up data offline.





# Art Crime

## The Case of the Stolen Stradivarius

When a 300-year-old Stradivarius violin valued at more than \$5 million was stolen from Milwaukee Symphony Orchestra concertmaster Frank Almond last year, investigators initially believed the theft may have been the work of sophisticated art thieves. The truth turned out to be much less glamorous.

Still, the tale of the theft and recovery of this rare instrument goes down in the annals of the FBI's Art Crime Team as a one-of-a-kind case.

the violin case discarded by the side of the road.

"There was an automatic assumption the violin would be traveling interstate and then most likely overseas," said Special Agent Dave Bass, a member of the Art Crime Team in the Bureau's Milwaukee Division.

Aware of the cultural significance of the violin—and that time was of the essence—the Milwaukee Police Department swiftly marshaled its forces and requested the FBI's assistance tracking down possible

resident Salah Salahaydn. A week after the robbery, Allah and Salahaydn were arrested and charged locally, but the violin and two valuable bows were still missing.

"One of my big concerns was how the violin was being stored," Bass said. Because the delicate instrument might be critically harmed by extreme cold or humidity, Bass and others were worried that it might be irreparably damaged.



The Lipinsky Stradivarius, shown here shortly after recovery, is 300 years old and valued at more than \$5 million.



Hours after the Stradivarius was stolen, Milwaukee Police Department officers found the violin's case discarded by the side of the road.

When Almond emerged from a back door of a concert hall at Wisconsin Lutheran College last January, where he had just performed, he was carrying the "Lipinski Strad"—made by Antonio Stradivari in 1715 and later named for the Polish violinist Karol Lipinski who played it. As Almond walked to his car, a man approached, pulled a Taser from his coat, and fired. With Almond temporarily incapacitated by the stun gun, the thief grabbed the Lipinski and fled to a waiting vehicle. Hours later, Milwaukee Police Department officers found

leads outside Wisconsin. Special Agents Tim Bisswurm and Brian Due began gathering information about the weapon used in the robbery, which led to one of the big breaks in the case.

Using evidence found at the crime scene, agents were able in a few days to trace the weapon from the manufacturer to the purchaser—a Milwaukee barber named Universal Knowledge Allah.

At the same time, with the investigation in high gear and a \$100,000 reward available, police received a tip regarding Milwaukee

Nine days after the robbery, Salahaydn led investigators to a Milwaukee home. With a borrowed ladder from the SWAT team, Bass climbed through a crawl space into the attic and retrieved the violin and the bows wrapped in a baby blanket inside an old suitcase.

"I am by no means a violin expert," Bass said, "but because of our training, I could make an informed opinion that in fact it was the Lipinski. And it appeared to be in great shape."

In May 2014, Allah pleaded guilty to felony robbery for his role in providing the stun gun to

Salahaydn. He is currently serving a three-and-a-half-year prison term. Last November, Salahaydn was sentenced to seven years in prison after earlier pleading guilty to the theft.

“My opinion is that the robbery was all about the reward money,” Bass said. “I believe Salahaydn’s intention was never to sell the violin. There are only a handful of people in the entire world who could do that, and he’s not one of them.”

lived. The crime was clearly premeditated.

Almond, who has been playing the Lipinski since 2008—on loan from an anonymous donor—was thrilled to get the violin back. “This was a fairly violent and traumatic event for me and my family,” he said recently. “But there were silver linings as well, in large part because of the unbelievable police work and cooperation between the Milwaukee Police Department and the FBI. I will be indebted to all of them for the rest of my life.”

playing the Lipinski for members of the Bureau, an FBI Citizens Academy group, and special guests from the Milwaukee Police Department.

Bass, a 10-year veteran of the Art Crime Team, explained that the Bureau worked “hand in hand” with the police department to support their case and added that he has never seen an armed robbery of an instrument of this value. “There are plenty of examples of theft—breaking into



The stolen violin was recovered in excellent condition.



Frank Almond thanked investigators in Milwaukee with a performance in December.

And nearly two decades earlier, Salahaydn was linked to a Milwaukee art theft and was later convicted of receiving stolen property after he tried to sell the stolen \$25,000 sculpture back to the gallery years after the crime.

In the end, Bass said, the Stradivarius robbery scheme was anything but sophisticated. The Taser was only good for one shot, and on a winter night when people wear heavy coats, it was more luck than skill that the weapon found its mark. Still, Salahaydn conducted extensive surveillance on Almond and knew where he and his family

When the violin was stolen, Almond said, “the community really came together and saw what kind of cultural treasure was in their midst.” Now, with all the publicity surrounding the case—and as the Lipinski celebrates its 300th birthday this year—he explained, “people want to hear the violin. There’s an interest in hearing the violin played live, and not just locally.”

Almond showed his gratitude last month to investigators who solved the case by taking part in a presentation at the FBI’s Milwaukee headquarters and

a practice room, or the musician accidentally leaves the instrument somewhere—but there has never been an instance I know of where someone walks up to one of these world-class musicians and forcibly takes an instrument. We hope that it never happens again.”



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/stolenstrad](http://www.fbi.gov/stolenstrad).



# Human Trafficking Ring Dismantled

## Case Highlights FBI's Commitment to Anti-Trafficking Efforts



The young Ukrainian men and women—many of them out of work and with few prospects—were promised good-paying jobs in the United States. But instead of living the American dream, they were thrust into a nightmare of violence, threats, and forced servitude.

For years, five brothers who ran a human trafficking organization victimized dozens of unwitting Ukrainians, underscoring the reality that modern-day slavery exists in the United States and around the world—and requires a strong response by governments and law enforcement.

In recognition of that fact, and to speak out for the victims, January has been declared National Slavery and Human Trafficking Prevention Month by the U.S. government. Human trafficking can take many forms, from forced servitude to sexual exploitation of children, and the FBI is fighting these crimes on every front.

The Botsvynyuk brothers created many victims. Based on trial transcripts and other public records, from approximately 2000 to 2007, the Ukrainians recruited their young countrymen to work in the U.S. in their businesses cleaning large retail stores at night. They promised good jobs, usually with salaries of \$500 per month. The victims were told that room

and board would be provided as well as all travel expenses. They were also told that they could earn \$10,000 after two or three years of working.

Many of those who signed up for these jobs were uneducated and desperate for work. “They believed it would be a much better deal than what they had in the Ukraine,” said Special Agent Ned Conway, who has been investigating this case out of our Philadelphia Division for nearly a decade.

Instead of entering the U.S. legally, many of the victims were smuggled through Mexico and ended up working 10- to 12-hour days, seven days a week. They lived up to five people in one room, slept on dirty mattresses on the floor, and most were never compensated—on the contrary, they were told they had to work for the brothers until their debts, ranging from \$10,000 to \$50,000, were paid.

Worse, the Botsvynyuks used physical force and sexual assault to keep victims enslaved. They also threatened violence to victims’ families still in the Ukraine.

“Some women were raped on their arrival in the U.S., and many of the men were beaten,” Conway said. “There was an element of fear right from the start.” Most of the victims didn’t speak English and felt they

had nowhere to turn. And they were afraid for their families back home.

Over time, though, some victims were detained at the border trying to gain entrance into the country, and other victims came forward. In 2010, all five brothers were indicted for human trafficking—specifically for conspiracy to violate the Racketeer Influenced and Corrupt Organizations (RICO) Act. Stepan and Omelyan Botsvynyuk were convicted in 2011, and in 2012, Stepan was sentenced to 20 years in prison. Omelyan received a life sentence.

Two other brothers, Mykhaylo and Yaroslav, fled to Canada. They were extradited in 2013, and their trial is set to begin this week in a Philadelphia federal court. The last brother, Dmytro Botsvynyuk, remains a fugitive in the Ukraine.

The damage caused by the Botsvynyuk brothers to perhaps 70 or more Ukrainian victims is staggering to contemplate. “The sexual assaults on the women were brutal,” Conway said, “and some of the men were psychologically broken. What happened to these innocent victims is a real tragedy. For some, their lives were destroyed.”

But there were a few bright spots to the story as well, Conway added. Some victims found the courage to testify against their abusers. And as victims of human trafficking, they also qualify for the right to apply for visas and stay in the U.S., which had been their dream all along.

“Without the brave cooperation of some of the victims,” Conway said, “it would have been more difficult to shut down the Botsvynyuks’ operation.”

# New Most Wanted Terrorist

## Naturalized U.S. Citizen Born in Somalia Added to FBI List

Liban Haji Mohamed, a naturalized U.S. citizen born in Somalia, has been named to the FBI's list of Most Wanted Terrorists, and a reward of up to \$50,000 is being offered for information leading to his arrest and conviction. Mohamed is charged with providing material support and resources to al Qaeda and al Shabaab, a Somali-based terrorist organization.

"Al Shabaab has claimed responsibility for many bombings in Somalia and Uganda and the 2013 attack on the Westgate Mall in Nairobi, Kenya," said Carl Ghattas, special agent in charge of the Counterterrorism Division at the FBI's Washington Field Office. "Liban Mohamed is believed to have left the U.S. with the intent to join al Shabaab in East Africa. We believe he is currently there operating on behalf of that terrorist organization."

Traveling with his U.S. passport, Mohamed is thought to have left the United States on or about July 5, 2012. Before his departure, the 29-year-old lived in the Northern Virginia suburbs of Washington, D.C., where he worked as a cab driver.

"While living in Northern Virginia, Mohamed was a recruiter and radicalizer for al Shabaab, which historically has targeted Westerners to go to Somalia and fight for them," Ghattas said. "Not only did Mohamed choose to go to Somalia and fight with al Shabaab, he took a prominent role in trying to recruit people and have them train with weapons."

A federal warrant for Mohamed's arrest was unsealed today by the U.S. Attorney's Office in the Eastern District of Virginia. In



addition to today's announcement adding Mohamed to the terrorist list and offering a reward for information leading to his arrest and conviction, the FBI is publicizing the case on social media channels in Somalia and elsewhere to encourage people to come forward with information about the fugitive.

"It is important for us to locate Mohamed because he has knowledge of the Washington, D.C. area's infrastructure such as shopping areas, Metro, airports, and government buildings," Ghattas explained. "This makes him an asset to his terrorist associates who might plot attacks on U.S. soil."

Shortly after leaving the U.S., the international police organization Interpol issued a blue notice for Mohamed to collect additional information about his identity, location, and activities. On August 15, 2014, Interpol issued a red notice to seek him as a wanted fugitive.

Mohamed speaks English, Somali, and Arabic. He is black, 6 feet tall, weighs about 194 pounds, and has black hair and brown eyes. He could be using aliases including Abu Ayrow, Shirwa, Shirwac,

Qatiluhum, and Qatil. Mohamed was a close associate of convicted terrorist Zachary Chesser, who was sentenced in 2011 to 25 years in prison for attempting to provide material support to al Shabaab.

There are currently 31 individuals on the FBI's Most Wanted Terrorists list. Those on the list have been charged in the U.S. for their alleged involvement in various terrorist attacks or planned attacks around the world against U.S. interests or persons.

The FBI also announced today it is seeking information about another individual, Ghazi Nasr Al-Din, regarding fundraising efforts on behalf of the terrorist group Hizballah.

Anyone with information about Liban Haji Mohamed or Ghazi Nasr Al-Din should contact the FBI or the nearest American Embassy or Consulate. Tips can be submitted anonymously online.

*Note: Liban Haji Mohamed and/or Ghazi Nasr Al-Din may have been located since this information was posted on our website. Please check [www.fbi.gov/wanted](http://www.fbi.gov/wanted) for up-to-date information.*



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/libanmohamed](http://www.fbi.gov/libanmohamed).



# Drug Kingpin Dethroned

## International Investigation Dismantles Criminal Enterprise



**Left:** The view from one of drug kingpin Alvaro Lopez Tardón's Miami condominium units, which overlooks another unit he owned in a nearby high-rise.

For years, Alvaro Lopez Tardón, a Spanish national, was living the high life in Miami—fancy cars, seaside condos, designer jewelry, and expensive leather goods. But it all came crashing down in the summer of 2011 when he was named in a U.S. federal money laundering indictment as the head of an international narcotics trafficking enterprise. His illicit enterprise was believed responsible for distributing more than 7,500 kilos of South American cocaine in Spain and laundering more than \$14 million in illegal drug proceeds in the United States.

Last fall, after being tried and convicted on numerous money laundering charges, Tardón was sentenced to an astonishing 150 years—exchanging his spacious South Beach penthouse for a small federal prison cell where he will spend the rest of his life. And in addition to the sentence, a \$14 million money judgment and a \$2 million fine were entered against him, and his assets are in the process of being forfeited.

Tardón made his initial mark in the drug trade back in the 1990s, when he—along with his brother Artemio—worked for a ruthless drug trafficker in Spain. By the early 2000s, the Tardón brothers

began a bloody feud with their boss and set about building their own criminal enterprise. They were ultimately successful—Alvaro directed the enterprise's illegal activities primarily from Miami, where he visited often, and second-in-command Artemio ran things from Madrid.

Here's how the money laundering scheme generally worked: the Tardóns' enterprise imported large quantities of Colombian cocaine from Peru into Spain. The illegal proceeds from the distribution and sale of the drugs would then be sent into the U.S., either carried by couriers or wire-transferred into any one of the numerous bank accounts Alvaro Tardón had set up (often not in his own name). He and his associates—usually through straw buyers or shell companies—would then launder the money through their purchases of luxury vehicles and high-end real estate in the Miami area.

By early 2011, though, the noose began to tighten around the Tardón organization. Spanish police raided a cocaine lab near Madrid run by a woman who distributed cocaine for the brothers. (Found at the lab were ledgers that matched ledgers later found in Alvaro's Miami penthouse.) By

July 2011, law enforcement in both countries had enough evidence to charge and arrest 20 members of the criminal group—16 individuals, including Artemio, in Madrid, and four, including Alvaro, in Miami.

Successfully investigating the activities of an international criminal organization requires the collaboration of law enforcement agencies at all levels, and that's exactly what happened in this case. From the very beginning of the investigation in 2010—when the Spanish National Police shared information about Alvaro and Artemio Tardón with the FBI through our Madrid Legal Attaché—Bureau investigators worked side by side with our partners internationally, with other U.S. federal agencies, and with local authorities in Florida.

An essential part of our money laundering case against Alvaro Tardón was an in-depth analysis of U.S. financial, real estate, and tax records as well as additional records shared with us by Spanish authorities. And Tardón's seven-week trial included the introduction of more than 36,000 pages of documents from Spain and the United States. Jurors also heard testimony from representatives of the Spanish National Police as well as Spain's national wiretapping agency and its taxing agency.

In the end, it was enough to convince a jury to convict Tardón and, according to Miami Special Agent in Charge George Piro, to ensure that “Alvaro Lopez Tardón's days as an international drug kingpin were over.”

# Former Los Alamos Lab Workers Sentenced

## Nuclear Scientist and Wife Passed Classified Documents

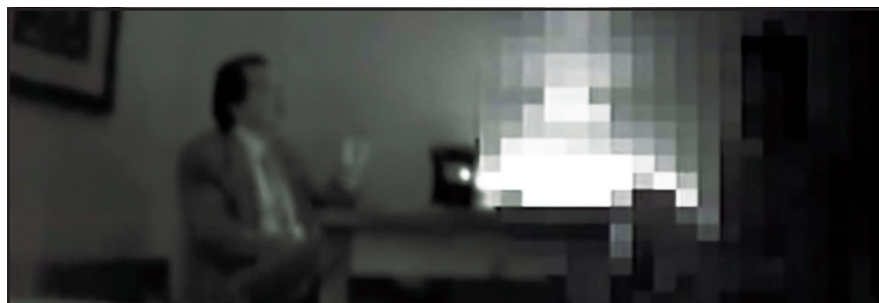
The reasons why he did it varied—he carried a grudge against his employer, he was frustrated with the U.S. government, he needed money, and he desired power and respect. But motivations aside, Pedro Leonardo Mascheroni, a scientist formerly employed at the Los Alamos National Laboratory in New Mexico, broke the law when he sold some of our nation's nuclear secrets to an individual he thought was a foreign government official. He also involved his wife—a Los Alamos employee at the time—in his illegal activities.

Both were charged and eventually pled guilty in connection with the plot. Last month, Pedro Mascheroni was sentenced to a federal prison term, while his wife—Marjorie Roxby Mascheroni—was sentenced last summer.

Pedro Mascheroni, a naturalized American citizen born in Argentina, had a Ph.D. in physics when he began working at Los Alamos in 1979. Los Alamos National Laboratory is one of several nuclear weapons labs in the country. During the majority of his time there, Mascheroni held a Department of Energy security clearance that allowed him access to certain classified information, including “restricted data,” a specific type of classified data dealing with nuclear weapons-related material. Marjorie Mascheroni, who worked as a technical writer and editor, had similar access.

In 1988, Pedro Mascheroni left Los Alamos as a result of a downsizing initiative, but Marjorie continued her employment with the lab.

Move ahead to the fall of 2007: Mascheroni, by his own admission,



**Pedro Mascheroni discusses nuclear weapons with an undercover agent he believed was a Venezuelan government official.**

contacted a Venezuelan official in the U.S. and offered his expertise and assistance to build a nuclear weapons program for that nation. That contact ultimately provided the FBI an opportunity to engage the scientist, in early 2008, through an undercover agent posing as a Venezuelan government official.

A note here: The indictment in this case did not allege that the government of Venezuela or anyone acting on its behalf sought or was passed any classified information, nor did it charge any Venezuelan government officials or anyone acting on their behalf with any wrongdoing.

In March 2008, Mascheroni had a series of discussions with our “Venezuelan government official” about his program to develop nuclear weapons for Venezuela. Among other things, he told the official/undercover agent that he could help Venezuela develop a nuclear bomb within 10 years and that, under this program, Venezuela could use a secret, underground nuclear reactor to produce and enrich plutonium and an open, above-ground reactor to produce nuclear energy. Mascheroni also asked our undercover agent about obtaining Venezuelan citizenship and explained how much he expected to be paid for his work.

Over the next year-and-a-half—

through e-mail, dead drops, and face-to-face meetings—Mascheroni passed to our agent documents he had written using classified and sometimes restricted data. During that time, he also received his first cash payment of \$20,000. Marjorie Mascheroni conspired with her husband by editing his written documents and occasionally accompanying him on dead drops and face-to-face meetings.

By October 2009, we had obtained enough evidence to search the Mascheronis' home, where we found several boxes of classified documents, sketches, plans, and notes—along with classified information on his computer—all from Los Alamos. Despite the fact that Pedro Mascheroni had left Los Alamos in 1988, the information, particularly the restricted data on nuclear weapons, was still relevant, still classified, and still harmful to U.S. national security if it fell into the wrong hands.

Special thanks to the Department of Energy and the Los Alamos National Laboratory for their assistance in this case, which serves as an example of the FBI's commitment to its mandate to expose, prevent, and investigate intelligence activities on U.S. soil.



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/mascheroni](http://www.fbi.gov/mascheroni).



# Art Crime Team Celebrates 10th Anniversary

## A Decade of Successful Investigations and Recoveries

To commemorate the 10th anniversary of the FBI's Art Crime Team, FBI.gov recently discussed the team's history, mission, and accomplishments with Bonnie Magness-Gardiner, who manages the Bureau's art theft program.

**Q:** How did the Art Crime Team get started?

**Magness-Gardiner:** The FBI has always had agents who investigated frauds and thefts related to art, but in 2003, there was substantial looting of Iraq's National Museum in Baghdad. Thousands of works were stolen. Because of the U.S. presence in Iraq at the time, it was clear that somebody would have to investigate. It was also clear that

the agent component has almost doubled to 15 men and women. One of the great benefits of having the agents located in so many cities in the U.S. is that we literally cover the country.

**Q:** Describe some of the team's accomplishments over the past decade.

**Magness-Gardiner:** One of our earliest successes was the recovery of a Rembrandt self-portrait valued at \$40 million. The painting had been stolen from the Swedish National Museum in Stockholm in 2000. We recovered it during an undercover operation in 2005. Since the Art Crime Team's creation, we have made more than

characteristics. Unlike automobiles, for example, art does not have a serial number on it. So we need specific descriptors that allow us to positively identify the works. Most submissions to the file come from local police departments or from victims. Currently there are about 8,000 listings, everything from fine art to collectibles—anything that has a cultural value that can be uniquely identified.

**Q:** Is there a particular kind of art that is more susceptible to being stolen or forged?

**Magness-Gardiner:** Unfortunately, it's an equal opportunity market for thieves and fraudsters. Over the last 10 years we have dealt with



*Fishing Boats Under the Cliff of Etretat, Claude Monet (missing)*



*Manhattan Moonlight, Ellison Hoover (missing)*



*Landscape on the Banks of the Seine, Pierre-Auguste Renoir (recovered)*

the U.S. government didn't have a team organized, in place, or with the expertise required to do that kind of investigation. But the need for such a team was apparent, and the FBI took that on. The Art Crime Team was formed a year or so later.

**Q:** What were those early days like?

**Magness-Gardiner:** When I first arrived, the team consisted of eight agents located in field offices around the country, as well as three trial attorneys from the Department of Justice assigned to assist with prosecutions. Today,

11,800 recoveries, and the value of those recovered objects is estimated to be more than \$160 million. We have also helped to convict more than 80 individuals for a range of art crimes.

**Q:** The National Stolen Art File has also been a success, hasn't it?

**Magness-Gardiner:** Yes, and particularly since it went online on FBI.gov in 2010. The National Stolen Art File is a database listing art stolen primarily in the United States. To be included in the file, the art must be valued at \$2,000 or more, and we require a theft report and a description of the work providing its unique

everything from fossils stolen from South America to modern art that's been forged and put on the market in New York. We have investigated cases involving fine art, manuscripts, letters, baseball cards, and textiles from pre-Colombian to modern. Everything that you can imagine that has a monetary value or cultural significance is subject to theft or fakery.

**Q:** Is investigating art crimes different from investigating other types of crimes?

**Magness-Gardiner:** Much of what we investigate is art theft, which is basically a theft of property. Most of our agents have a background

in investigating property theft and interstate transportation of stolen property. So in one sense they are using time-tested investigative methods. It's the objects they are dealing with that make these cases special. The items are often fragile, so if they are recovered they must be handled with special techniques. We also have to determine if they are authentic. Is this actually the work we are looking for, or is this a forgery?

**Q:** What kinds of agents are drawn to the Art Crime Team and what backgrounds do they have?

**Magness-Gardiner:** Some of our agents have a fine art or art history background, or are themselves

we are also a market for illicit art that is being brought in from other countries. Sometimes the works are stolen from collections, while much of it—artifacts and antiquities—is looted directly out of the ground, which complicates things because often there is no record of it. Objects might come from archeological sites or from poorly inventoried churches and monasteries. These objects, whether in museums, other collections, or in the ground, can be very valuable in a monetary sense, and in their countries of origin they have an even greater value as cultural heritage.

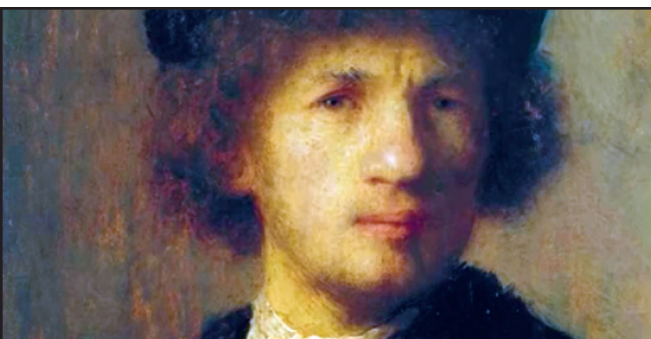
**Q:** So the Art Crime Team works

country of origin.

**Magness-Gardiner:** It is very satisfying to return things to people, whether to individual victims, institutions, or countries. Many of these objects have great personal significance, and huge institutional significance when a museum or archive is involved. When a country gets something returned, of course this has a great deal of meaning. People are very grateful for our help. We have been very successful in these areas.

**Q:** And to what do you owe that success?

**Magness-Gardiner:** A big part of our success is the team approach,



**Self-Portrait,**  
Rembrandt H. van Rijn (recovered)

**National Stolen Art File (NSAF)**



**Bonnie Magness-Gardiner describes**  
the FBI's Art Crime Team.

artists or collectors. But that's fewer than half of the individuals on the team. The other members have an interest in art, culture, and history—and to my point of view, that is just as significant—and being on the team allows them to expand their knowledge while doing good by investigating thefts or frauds in these areas.

**Q:** How serious a problem is art crime?

**Magness-Gardiner:** Here in the U.S., we are a market for all sorts of art. There is a big community of collectors, museums, and dealers. But because we are such a big market for legitimate art,

closely with international law enforcement and other countries?

**Magness-Gardiner:** Yes. More than half of our cases have some international element. But we also work closely with our domestic law enforcement partners and with the art community in general. We work with foreign governments to identify stolen pieces and attempt to recover them when we can find them in the United States. These are usually items that relate to the history and ethnicity of that culture. When these things are lost, a culture is made poorer for it.

**Q:** It must be gratifying to return items of such significance to their

because it allows us to work throughout the entire country with a highly trained group of individuals who communicate with each other and are passionate—and determined—about the work they do.

*Note: The art depicted here may have been recovered since this information was posted on our website. Please check the National Stolen Art File at [www.fbi.gov/nsaf](http://www.fbi.gov/nsaf) for up-to-date information.*



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/artcrimeteam10years](http://www.fbi.gov/artcrimeteam10years).



# Law Enforcement and Race

## Director Cites ‘Hard Truths’ and Calls for ‘Open Discussion’

FBI Director James B. Comey called on the nation’s law enforcement personnel and the citizens they serve to participate in a frank and open conversation about the disconnect that exists in places like New York City and Ferguson, Missouri—and many communities across the country—between police agencies and many citizens, particularly in communities of color.

In a speech today at Georgetown University, Comey said the lethal police encounters involving Michael Brown and Eric Garner, the ensuing protests across the country, and the assassinations of New York Police Department Officers Wenjian Liu and Rafael Ramos have put the fundamental relationship between police and their constituents at a crossroads.

“As a society, we can choose to live our everyday lives, raising our families and going to work, hoping someone, somewhere, will do something to ease the tension,” Comey said. “We can turn up the music on the car radio and drive around these problems. Or we can choose to have an open and honest discussion about what our relationship is today—what it should be, what it could be, and what it needs to be—if we took more time to better understand one another.”

The speech, entitled “Hard Truths: Law Enforcement and Race,” sought to move the ongoing debate about race and the character of law enforcement officers to a more productive footing, where police and citizens acknowledge a few elemental “truths” in an effort to better understand each other. The Director began by acknowledging law enforcement’s own spotty history, including



**Director Comey addresses students and faculty at Georgetown University. Seated is Edward Montgomery, dean of the university's McCourt School of Public Policy, which co-hosted the event.**

police bias a century ago against Irish immigrants—from whom Comey descended—and the FBI’s surveillance of civil rights leader Dr. Martin Luther King, Jr.

“At many points in American history, law enforcement enforced...a status quo that was often brutally unfair to disfavored groups,” Comey said. “One reason we cannot forget our law enforcement legacy is that the people we serve cannot forget it either. So we must talk about our history. It is a hard truth that lives on.”

Comey raised the subject of the unconscious racial bias within all of us, but said it’s how we behave in response that defines us. He said racial bias is no more prevalent in law enforcement than anywhere else. “In fact,” he said, “I believe law enforcement overwhelmingly attracts people who want to do good for a living. They don’t sign up to be cops in New York or Chicago or L.A. because they want to help white people or black people or Hispanic people or Asian people. They sign up because they want to help all people.”

That being said, many police over time develop different flavors of cynicism—lazy mental shortcuts, Comey said, that we have to

resist because they can lead to over-generalizing. “We need to come to grips with the fact that this behavior complicates the relationship between police and the communities they serve.”

Still another hard truth, Comey added, is the recognition and need to address the disproportionate challenges faced by young black men in struggling communities—inadequate education, jobs, and role models. Too often, he said, they inherit a legacy of crime and prison. “Changing that legacy is a challenge so enormous and so complicated that it is, unfortunately, easier to talk only about the cops,” Comey said. “And that’s not fair.”

Comey said law enforcement needs to better “see” the people they serve. And to that end, he is urging police departments to provide the FBI with better, more complete data, such as demographics and circumstances, which could shine more light on incidents where force is used by police or against them.

But the “seeing” needs to flow both ways. Citizens need to understand the difficult and perilous work of law enforcement. “If they take the time to do that, what they will see are officers who are human, who are overwhelmingly doing the right thing for the right reasons,” he said.

“We all need to talk and we all need to listen,” Comey said in closing, “not just about easy things but about hard things, too. It is time to start seeing one another for who and what we really are.”



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/lawenforcementandrace](http://www.fbi.gov/lawenforcementandrace).

# A Ponzi Scheme Collapses

## Financial Crime Ring Uncovered, Criminals Brought to Justice

Nearly a dozen fraudsters who conspired to operate a \$40 million Ponzi scheme will be spending plenty of time behind bars after a joint effort by the FBI, the Internal Revenue Service, and the U.S. Attorney's Office in the Western District of North Carolina. Among those now serving time is the scheme's mastermind, Keith Franklin Simmons, who was sentenced to 40 years in prison late last year. And just last month, the 11th and final defendant in the conspiracy—Jonathan D. Davey—was sentenced to more than 21 years.

The federal judge who sentenced Davey said the term handed down reflected the effects of the fraud on its 400 or so victims—mainly elderly and vulnerable—and that the scheme resulted in “life-wrecking damage” and caused victims to lose “life savings, trust, faith, and their sense of dignity.”

In 2007, Simmons—a North Carolina businessman looking for a way to make easy money—formulated an investment scheme called “Black Diamond,” which he advertised as a legitimate hedge fund involved in foreign currency trading. Black Diamond, according to Simmons, had significant safeguards in place to protect investors, was independently audited, and had consistently high rates of return. None of that, of course, was true.

To help solicit investors from around the country, Simmons—through a co-conspirator—recruited a number of individuals to serve as regional managers of his hedge fund. Most of these “managers” had insurance experience and were well versed in selling annuity products, often to the



**The modest North Carolina office building where businessman Keith Franklin Simmons orchestrated his \$40 million Ponzi scheme.**

elderly. So they solicited previous customers—as well as friends, family, and acquaintances. These early investors were promised financial compensation for bringing new investors on board, so they in turn praised Black Diamond and its high rate of return to their friends, family, and acquaintances. Unfortunately, not a single dollar of investor funds was actually invested.

Also brought on board to oversee the various hedge fund managers—and the money—was Davey, a certified public accountant and investment manager in Ohio. Davey controlled most of the funds from the scheme and published a website for investors that reflected false returns. By the end of the scheme, the website showed that the value of investor accounts was more than \$120 million, but in reality, all of the accounts totaled less than \$1 million.

Black Diamond made the perpetrators—in particular Simmons and Davey—very rich. And as long as new money was coming in, they were able to keep making some payments to their early investors while at the same time continuing to fund their lavish lifestyles, which included mansions, luxury vehicles, and expensive trips.

But as all Ponzi schemes usually do at some point, Black Diamond began to collapse in on itself—there was not enough new money coming in to keep the old investors satisfied or to continue lining the pockets of the criminals running the fraud. So around March 2009, a new Ponzi scheme was begun, but this time some of the money from investors in the new scheme went to make payments to the investors of the old scheme, and the rest went to the criminals.

It was the beginning of the end, however. Acting on allegations of suspicious financial activity, the FBI—with its partners—was already investigating Black Diamond. By December 2009, ringleader Keith Franklin Simmons was in custody, and the arrests of his co-conspirators eventually followed.

### **Don't Let a Ponzi Schemer Victimize You**

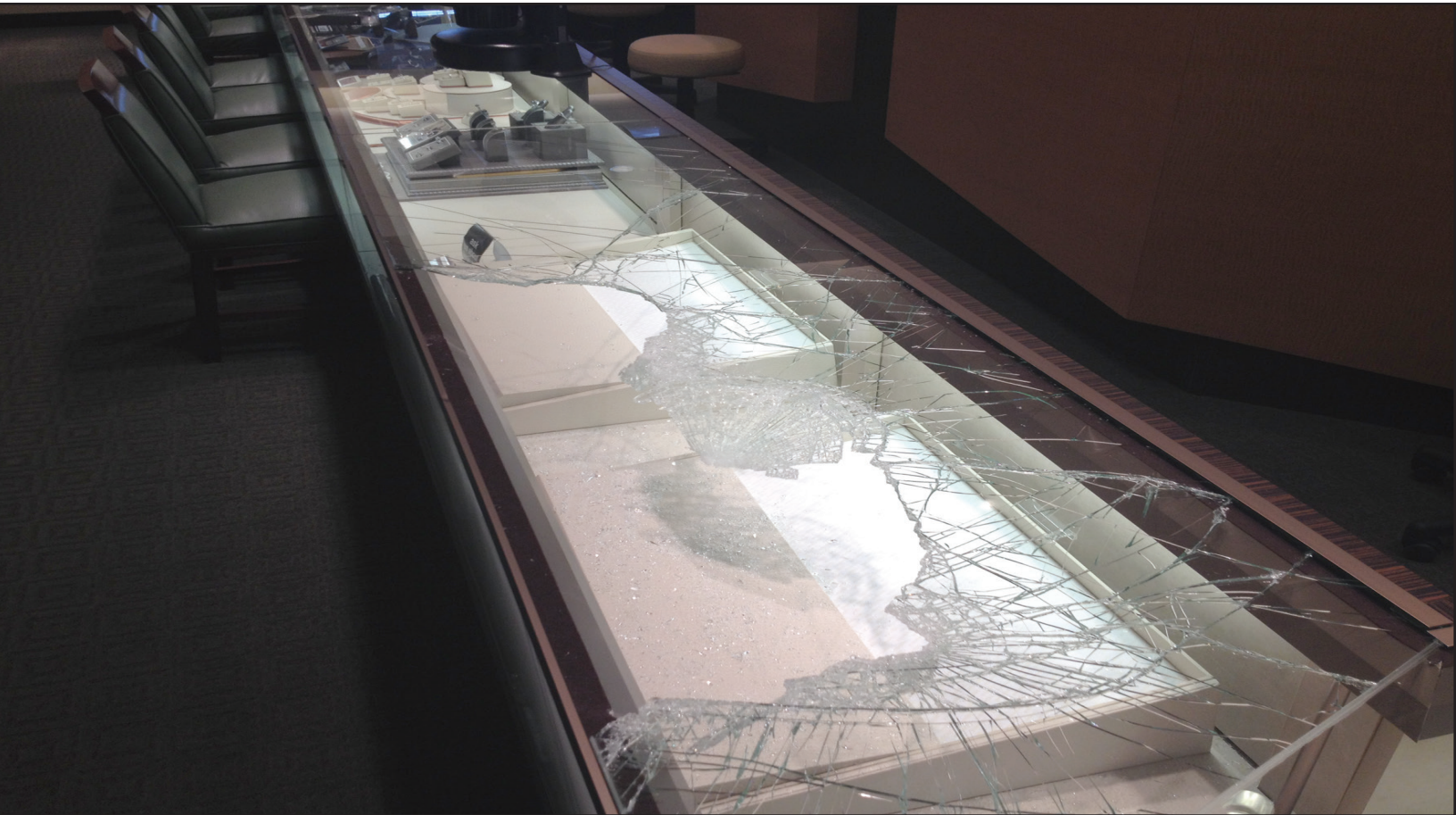
Today's financial scams are often more sophisticated than ever before. Here are a few tips to help you avoid becoming the victim of a Ponzi scheme:

- Be careful of any investment opportunity that makes exaggerated earnings claims.
- Don't be fooled into believing an investment is safe just because someone you know recommended it. So-called “affinity scams” are one of the favorite methods used to lure people into Ponzi schemes.
- Exercise due diligence in selecting investments and the people with whom you invest—in other words, do your homework.
- Consult an unbiased third party, like an unconnected broker or licensed financial adviser, before investing.
- Take the time to check out investment offers by contacting your state's securities regulator.
- Never put all of your eggs (investments) in one basket.



# Joint Effort Takes Down Detroit-Based Robbery Group

But Smash and Grab Jewelry Store Incidents are on the Rise



Shown are the remains of a glass display case after a smash and grab robbery of a jewelry store. According to the Jewelers' Security Alliance, the number of smash and grab robberies is on the rise nationwide.

Today, the FBI and its partners announced three separate indictments filed during the past month against 17 individuals from the metropolitan Detroit area who are believed to be responsible for a number of “smash and grab” robberies of jewelry stores in a half-dozen states. The charges, filed in federal court in the Eastern District of Michigan, involved violations of the Hobbs Act, which makes it a crime to obstruct, delay, or affect interstate commerce by robbery.

The indictments follow a series of investigations around the nation by various local, state, and federal law enforcement agencies involving approximately 40 smash and grab jewelry store robberies. Authorities

also announced they are looking for the public's help in identifying 16 other individuals believed to be connected to additional smash and grab robberies.

*There were 110 smash and grabs during 2014, nearly twice the number (62) reported during 2013.*

Smash and grab robberies are aptly named—they involve perpetrators who enter a jewelry store and, in front of store employees and customers alike, threateningly whip out tools like sledgehammers, smash those hammers through the glass displays, and grab expensive pieces of jewelry before taking off,

stunning and frightening anyone who witnesses their actions. In addition to the constant threat of violence from these criminals, there have been instances of innocent bystanders actually getting hurt during these robberies.

And unfortunately, these types of robberies around the nation have recently increased at an alarming rate.

According to the Jewelers' Security Alliance (JSA)—a non-profit group that provides crime information and assistance to the jewelry industry and law enforcement—there were 110 smash and grabs during 2014, nearly twice the number (62) reported during 2013.

And once the jewelry is stolen, it's relatively easy to transport it to whichever fence the criminals do business with so it can be quickly sold for cash—which can then be used to fuel other crimes the groups may be committing.

At first glance, these robberies seem like local crimes, so why is the FBI even involved? For several reasons: First, because often times, the stolen merchandise crosses state—and sometimes national—borders, so a federal law enforcement agency with offices around the nation and even overseas is vital; second, because the robberies are being increasingly committed by organized criminal enterprises that operate in multiple jurisdictions; and lastly, because these crime groups are often involved in other kinds of organized crime activity that the FBI is already investigating.

But of course we can't—and don't—do it alone. The investigation that resulted in the

Detroit indictments was conducted by the multi-agency, FBI-led Oakland County Gang and Violent Crime Task Force and involved coordination among multiple Bureau field offices, state and local law enforcement agencies around the country, and our private partners in the jewelry industry. That coordination—the sharing of vital information, methods of operation, and evidence—is what allowed us to link the robberies to the same criminal crew.

Explains John Kennedy, head of the Jewelers' Security Alliance, which represents the interests of 21,000 retail jewelry stores, "It's very difficult for a local agency to address the problem by itself, but when the FBI—with its national and international scope—assists, the overall law enforcement effort is more effective." The JSA also plays a key role in these investigations by offering law enforcement agencies access to its database of jewelry and gem thefts.

The fallout from these smash and grab robberies can be seen across the board. Obviously, store employees and customers are traumatized when faced with the threat of violence. Jewelry stores suffer tremendous losses, as do the insurance companies who must pay the resulting claims. Stores also spend additional money to enhance their security measures—hiring security guards, upgrading the strength of their display cases, installing or augmenting video monitoring equipment, etc. And eventually, over time, the fallout could hit the public at large, with higher insurance costs and higher prices at the jewelry store.

But by combining the most effective resources, tools, and expertise, law enforcement and prosecutors—along with our private sector partners—are teaming up to identify those responsible for these violent crimes and put them behind bars.

### In Their Own Words

Our state and local partners played a vital role in this Detroit investigation into a criminal enterprise allegedly engaging in a series of smash and grab jewelry store robberies. But that's nothing unique—on daily basis, the FBI works with our state and local partners around the country on all sorts of criminal and national security cases. Here are some reflections on the importance of law enforcement cooperation from several of the agencies involved in the Detroit case.

*"When violent acts like these are committed in places where families shop and do other business, it becomes even more imperative to get these suspects behind bars. We're working with other partner agencies to capture these individuals who are jeopardizing the safety of Loudoun residents, and to prevent future confrontations with the public."*

- Sheriff Michael L. Chapman, Loudoun County, Virginia

*"It's the goal of the Michigan State Police to work collaboratively with our law enforcement partners, and these types of crimes [smash and grabs] have the potential to be violent, which impacts public safety. We are proud to be a part of this investigation which will make our citizens feel safe again during their daily routines."*

- Captain Monica Yesh, Michigan State Police

*"Joining our resources with those of the FBI has enhanced our effectiveness by allowing their long-arm jurisdictional reach to cross state lines in pursuit of these dangerous criminals. Our partnership with the Bureau has resulted in a more effective consolidated quest to arrest and prosecute these violent perpetrators."*

- Chief Bart Aguirre, Tupelo (Mississippi) Police Department



# License to Steal

## Multi-State Fraudulent Document Ring Dismantled

For the hundreds of individuals living in the United States illegally who responded to advertisements by Young-Kyu Park and his associates, the promise of an authentic visa or a valid driver's license was well worth the \$3,000 to \$4,500 price tag.

Park, who was recently sentenced to six years in federal prison, was the leader of a multi-state criminal organization that fraudulently obtained driver's licenses and other documents such as student visas for illegal aliens and other ineligible individuals.

In New Jersey, New York, California, Nevada, Virginia, and Georgia between 2010 and 2012, "it was open season for driver's licenses," said Special Agent Theresa Fanelli. "Park was willing to sell to whoever wanted to buy." In Las Vegas, his associates even operated a shuttle service to take clients to the Department of Motor Vehicles to obtain a license using their bogus credentials. And with that valid license, individuals had a key piece of identification that enabled them to access other services previously unavailable to them.

Park was one of 22 people charged in 2012 with providing a range of illegal services predominantly to South Koreans who were illegally residing in the U.S. He was assisted in his criminal enterprise by brokers he employed around the country, along with a contract employee of the U.S. Citizenship and Immigration Services (USCIS), who stole authentic forms that turned out to be central to the scheme.

Through a third party, Park was able to obtain I-797 forms from USCIS employee Martin

Trejo. The form is used by the federal government to convey an immigration benefit. For example, state agencies that issue driver's licenses rely on the I-797 form to verify the authenticity of an applicant's foreign passport and lawful presence in the U.S.

***"He purposely exploited vulnerabilities in the immigration and motor vehicle process to line his own pockets."***

During the investigation into Park, it was determined that the I-797 forms being used illegally were not counterfeit. "We knew someone on the inside had to be selling the forms, because the public has no way to access them," said Special Agent Nathan Kim, who, along with Fanelli, investigated the case out of our Newark Division.

The evidence led to Trejo, who was arrested and charged with conspiracy to steal government property and interstate transportation of stolen goods. In September 2014, he was sentenced to 26 months in prison.

Trejo, who had worked at a USCIS warehouse in California for more than a decade, estimated that he stole about 1,000 forms to make extra money, Kim said. "The form center has since made numerous changes to mitigate the problem and secure these forms."

**Left: Federal I-797 forms—like this one—stolen from a U.S. Citizenship and Immigration Services facility in California helped a criminal organization fraudulently obtain driver's licenses and visas for hundreds of individuals living in the United States illegally.**

During the nearly 18-month investigation, Fanelli said that Park and his associates helped hundreds of individuals obtain fraudulent driver's licenses. "He would also provide supporting paperwork, fabricating documents to show proof of residence, bank statements—whatever you needed."

His customers—many were arrested and charged with state violations—"knew they didn't have legal status," Fanelli explained, adding that state motor vehicle offices were exceptionally helpful during the investigation.

Park pled guilty to several charges, including producing false identification documents, conspiracy to steal government property, and money laundering. When his prison term is up, he will be deported to South Korea.

"He always claimed that he was a Robin Hood of the community, helping people who had no other alternatives," Fanelli said. "Of course, he was benefiting handsomely and living in high style." She added, "Park knew what he was doing was illegal. He purposely exploited vulnerabilities in the immigration and motor vehicle process to line his own pockets."

# The Cyber Action Team

## Rapidly Responding to Major Computer Intrusions

It can be a company's worst nightmare—the discovery that hackers have infiltrated their computer networks and made off with trade secrets, customers' personal information, and other critical data.

When such intrusions happen—and unfortunately, they occur frequently—the FBI can respond with a range of investigative assets, including the little-known Cyber Action Team (CAT). This rapid deployment group of cyber experts can be on the scene just about anywhere in the world within 48 hours, providing investigative support and helping to answer critical questions that can quickly move a case forward.

“Our goal is to provide information that can be actioned immediately,” said Special Agent Chris Lamb, a CAT member since 2007. “A lot of the evidence in a cyber intrusion may only be there for a little while,” he said. “The trail can get cold pretty quickly.”

Established by the FBI's Cyber Division in 2006 to provide rapid incident response on major computer intrusions and cyber-related emergencies, the team has approximately 50 members located in field offices around the country. They are either special agents or computer scientists, and all possess advanced training in computer languages, forensic investigations, and malware analysis.

“I call it speaking geek,” said Lamb, describing the skills CAT members must possess and maintain to be on the team. “You could compare it to an English speaker trying to learn Mandarin Chinese. You have to spend years immersing yourself in the language to become fluent. And then you have to keep



practicing. But unlike Mandarin, which basically stays the same, the challenge for us is that the language of cyber is constantly changing.”

***This rapid deployment group of cyber experts can be on the scene just about anywhere in the world within 48 hours.***

Since the Cyber Action Team's inception, the FBI has investigated hundreds of cyber crimes. More than 50 of those cases were deemed of such significance that the rapid response and specialized skills of the Cyber Action Team were required. Some of those cases affected U.S. interests abroad, and the team deployed overseas, working through our legal attaché offices and with our international partners.

“Our job is to very quickly understand what the bad guy did and why,” said Lamb, who works out of our Kansas City Division. “We make an initial assessment to determine what we know and

what we don't know. Based on that assessment, we then call in other experts to fill whatever gaps we need to have filled.”

“Using cutting-edge tools, we look for a hacker's signature,” he explained. In the cyber world, such signatures are called TTPs—tools, techniques, and procedures. The TTPs usually point to a specific group or person. The hackers may represent a criminal enterprise looking for financial gain or state-sponsored entities seeking a strategic advantage over the U.S.

Either way, victim companies are often surprised by how much of their networks have been compromised—and for how long. Some intrusions are not discovered until months or even years after the fact.

Hackers have become so sophisticated that they can overcome even the best network security measures, he noted. “We tell victims that it sometimes doesn't matter how good your security is, the bad guys can still get in.”



# Law Enforcement and Race

## Continuing the Conversation

The sometimes uneasy relationship between members of law enforcement and the diverse communities they serve can be a difficult topic to discuss, but FBI Director James B. Comey today encouraged the National Organization of Black Law Enforcement Executives (NOBLE) to continue that conversation—and he again called for better reporting of incidents where force is used by police and against them.

During a speech to the NOBLE group in Atlanta, Georgia, Comey noted that the organization's members were "uniquely qualified as law enforcement leaders who are leaders of color" to drive this conversation forward, and he pledged that the FBI would strive to be a more diverse organization to reflect the nation it serves.

In the wake of the death of Michael Brown in Ferguson, Missouri, the assassinations of two New York City Police Department officers, and other recent racially charged police incidents around the country, Comey last month publicly addressed the contentious issue of law enforcement and race, acknowledging some "hard truths."

"One of my worries is that we were drifting to a place where we were not having a balanced conversation," Comey said, and not being honest about how law enforcement and ethnic communities "see" one another. He called on NOBLE members to help "foster a more balanced and open-minded discussion."

One of Comey's goals is to have better reporting of data about encounters between police and citizens, especially violent encounters. Currently, demographic data regarding officer-involved



**Director Comey's remarks to the National Organization of Black Law Enforcement Executives touched on diversity, terrorism, and the need for better reporting of incidents where force is used by police and against them.**

shootings is not consistently reported to the FBI through its Uniform Crime Reporting Program because reporting is voluntary for local police departments. "In the absence of that data," he said, "all conversations about policing and policy are uninformed, and that's not a good place to be. We can do better."

On the issue of diversity within the FBI, Comey acknowledged that the number of minority special agents has been on a slow but steady decline, and he is working on new recruiting strategies to hire more people of color.

"Diversity must be at the core of all of our conversations at the FBI," he said. "Diversity is about doing the right thing, but also about effectiveness. It's about being good at what we do. We are simply less effective when we are less diverse."

A more diverse workforce allows the Bureau to connect better to the communities it serves and fosters greater trust with witnesses, victims, and even potential sources. "Diversity gives us credibility," he explained, adding that he recently added diversity to the list of the FBI's core values. "I want to talk about it and drive it into the conversations we have in my organization every single day."

Cedric Alexander, president of NOBLE, said he appreciated Comey's candor regarding the issue of law enforcement and race. "His willingness to be part of change in a positive way—and seeking out NOBLE to work with him and take an active role in creating a better public safety environment at all levels—is admirable. He has obviously given a lot of thought to these issues."

Comey also spoke about the changing terrorism threat and why partnership between local, state, and federal law enforcement is in many ways more critical now than it was after the 9/11 attacks.

"We have taken the fight to core al Qaeda," he said, and largely diminished their capacity to strike America. But spinoff groups such as ISIL have gotten "very slick at social media" and are spreading a poisonous message through the Internet. "ISIL is issuing a siren song to troubled souls," he explained, and these homegrown terrorists are more likely to be initially noticed by a police officer on a neighborhood patrol than a federal officer.

The homegrown terror threat is occurring everywhere in the country, Comey said. "In all 50 states, there are people who are in some stage of consuming this propaganda and moving toward radicalization. Our task is to find them and disrupt them." The only way to succeed at that, he added, is through a unified law enforcement effort.



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/continuingtheconversation](http://www.fbi.gov/continuingtheconversation).

# Financial Fraud

## Hollywood Film Scheme Results in Unhappy Ending for Investors

The owners of Gigapix Studios told investors they had a sure thing: They were going to make an animated version of the *Wizard of Oz* called *OZ3D*, and those who got in on the ground floor—and the company’s imminent public offering—could make a killing.

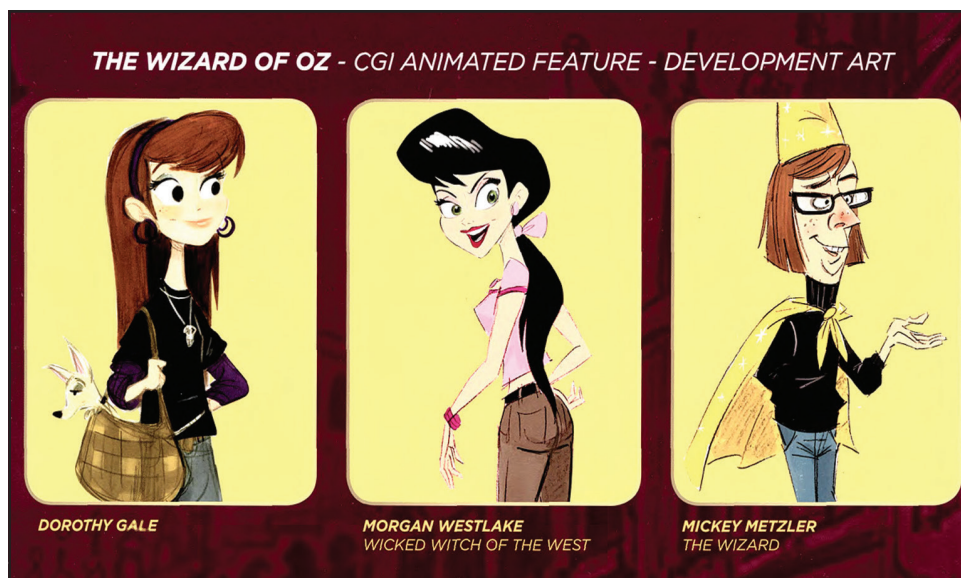
Unfortunately, the film was a bigger fairy tale than investors bargained for, and approximately 730 people lost millions of dollars. For some, the investment represented their life savings.

“Potential investors were told, ‘You’re going to make so much money that your kids and grandkids won’t want for anything,’” said Special Agent Eric Potocek, who investigated the case out of our Los Angeles Division. “In the end, the movie was never made, and it is unlikely investors will ever get anything back.”

Between the film and the impending public offering, the two principal fraudsters behind Los Angeles-based Gigapix raised some \$21 million over a seven-year period beginning in 2006. Of the \$8 million raised for the movie, only 5 percent of that amount went toward actually producing a film. The rest was used to pay big salaries, commissions, overhead for a fancy office, and other expenses.

Christopher Blauvelt, 59, and David Pritchard, 67, were convicted in 2014 on a series of federal charges including mail fraud, wire fraud, and offering unregistered securities for sale. Last month, Blauvelt was sentenced to eight years in prison, and Pritchard received a five-year term.

Blauvelt founded Gigapix in 2002 and brought Pritchard on as a partner four years later. The two hired telemarketers to solicit



Development art depicting characters in the movie *OZ3D*—an animated version of the *Wizard of Oz*—which was never made by Gigapix Studios even after hundreds of victims were lured into investing millions of dollars in the project.

potential investors, who were told that Gigapix was a blockbuster animation company waiting to happen—similar to Pixar Animation Studios—and that Gigapix was developing projects expected to generate huge profits when the company went public.

The telemarketers—known as “fronters”—used marketing lists to cold call potential investors and worked from scripts touting the supposed merits of Gigapix. When victims expressed an interest in investing, they were turned over to “closers” who collected their money. Two of the company’s closers were also convicted in the fraud.

While soliciting money for Gigapix and *OZ3D*, the defendants told lies and half-truths, suggesting that the company was financially successful and investors would receive high returns on their investments in less than 18 months. They claimed that investments carried little or no risk.

Some of the victims were “savvy investors,” Potocek noted, and perhaps could afford to lose what

they risked. But many victims—referred by friends or other investors and who lived far away from Hollywood—were susceptible to the sales pitch and the lure of being part of the film business.

“Many of the victims were not wealthy people,” Potocek said. “They were teachers and secretaries and folks who worked 30 or 40 years to save for retirement.” He added that Gigapix “took money from older people and from others who clearly could not afford to lose it. People lost their homes and had their dreams of retiring evaporate.”

There have been other recent cases in Los Angeles involving movie fraud, where telemarketers lure victims into investing in films that never get made. “These criminals were selling entertainment,” Potocek said, “but it could just as easily have been stocks or precious metals. When someone promises a high rate of return in a very short time, and with little or no risk, any investor should beware. Those are very large red flags.”



# Leader of Violent Street Gang Going to Prison

## Multi-Agency Investigation Dismantles Criminal Organization

He headed a dangerous criminal organization responsible for not only a great deal of the gang violence occurring on the streets of New Haven, Connecticut, but also for the large-scale distribution of cocaine in and around the city. But earlier this month, Donald “Main” Ogman was sentenced to more than 15 years in prison after pleading guilty to federal drug charges. Nineteen of his fellow gang members and other associates have previously pled guilty to various federal charges.

And as a result, the streets of New Haven are a little safer these days.

Under Ogman’s leadership, his criminal enterprise—the Grape Street Crips—was a force to be reckoned with. Much of the violence—a lot of it in the Hill neighborhood of New Haven—was attributed to the turf battle occurring between the Crips and other gangs. The Grape Street Crips wanted to maintain their influence over drug trafficking and firearms trafficking in the Hill, and they used intimidation, threats of violence, shootings, assaults, and homicides to make sure that they did.

But Ogman also had a direct hand in the trafficking of drugs—he would purchase large quantities of cocaine from criminal suppliers, and then, after processing the cocaine into “crack,” redistribute it to gang members and others in the Hill and other neighborhoods. Ogman often cooked the cocaine into crack himself and used drug addicts (or “friends,” as he called them) to test the batches he made.

Trying to get a handle on the drug trafficking and violence being perpetrated by the Grape Street Crips and other gangs, the



**In March 2012, during an investigation into the Grape Street Crips, members of the New Haven Safe Streets Task Force executed a number of search warrants, including one for the above residence of the gang’s leader, Donald Ogman. Investigators found crack cocaine, drug paraphernalia, and other illegal items.**

FBI’s New Haven Safe Streets Task Force—which includes the Connecticut Department of Corrections, the Connecticut State Police, and the New Haven, Hamden, and Milford Police Departments—began to investigate and soon honed in on Ogman and his associates.

The FBI has 164 Violent Gang Safe Streets Task Forces in field offices nationwide, staffed by nearly 850 Bureau agents, more than 1,500 state and local law enforcement personnel, and almost 100 other federal law enforcement agents. These task forces go after violent gangs through sustained, proactive, coordinated investigations—often using federal laws targeting racketeering, drug conspiracy, and firearms violations to identify and prosecute the leadership of these gangs and obtain lengthy prison sentences. Our Safe Streets initiative is the principal federal, state, and local partnership engaged in reducing violent crime throughout the country.

For the investigation into Donald Ogman and the Grape Street Crips, Bureau agents and task force officers working side by side used a variety of techniques to uncover the extent of the group’s criminal activity, including court-authorized wiretaps, the execution of search and seizure warrants, electronic and physical surveillance, and confidential informants. Between March and September 2011, law enforcement also set up a series of about 75 controlled drug buys—using confidential informants to purchase cocaine from members and associates of the gang, including Ogman.

The wiretaps on Ogman’s phone were fruitful as well, providing evidence of his leadership of the Grape Street Crips and his involvement in drug trafficking. During one particular conversation he had with an associate, the two discussed a couple of unrelated federal drug investigations in New Haven and mused on the perils of being the target of such an investigation.

Ogman soon found out how perilous it could be. In March 2012, investigators executed a series of search warrants, seizing drugs, drug paraphernalia, cash, firearms, ammunition, and other items. Ogman was charged and taken into custody, as were a number of his fellow gang members and associates. In March 2014, he pled guilty to drug conspiracy charges prior to his sentencing.

And not long after Ogman was taken into custody and his criminal enterprise was virtually dismantled, New Haven police reportedly noted a reduction in crime in the neighborhood areas where the Grape Street Crips operated.

# Progress Report

## Panel Conducts Review of FBI Since 9/11 Commission Report

A congressionally mandated panel charged with reviewing the FBI's implementation of recommendations contained in the *9/11 Commission Report* in 2004 today issued its findings.

The release of the 9/11 Review Commission's report, *The FBI: Protecting the Homeland in the 21st Century*, followed 14 months of research, interviews, briefings, and field visits by commissioners and their 13-member staff. The commission—which included former Attorney General Edwin Meese, former Congressman Tim Roemer, and Georgetown University professor Bruce Hoffman—began its review in 2013 at the FBI's request after Congress called for an appraisal of the Bureau's progress since the 9/11 Commission issued its recommendations in 2004. A classified draft of the Review Commission's report was sent to Congress and to other agencies mentioned in the report; the FBI released the unclassified version for the public.

That report, which can be found on [FBI.gov](http://FBI.gov), concludes that the FBI has “transformed itself over the last 10 years” and “made measurable progress building a threat-based, intelligence-driven national security organization.” The commission also makes recommendations on where the FBI can improve.

In a press briefing today at FBI Headquarters, Director James B. Comey was joined by the report's commissioners to discuss the findings.

“This has been a tremendously valuable thing to me as a new Director,” Comey told reporters. “My take, I can divide it into three buckets: Overwhelmingly,



Director Comey listens as former Attorney General Edwin Meese discusses the findings of the 9/11 Review Commission. Meese, along with Georgetown University professor Bruce Hoffman (far left) and former Congressman Tim Roemer (far right) comprised the commission.

I agree with their findings and their recommendations; there's a small group that I need to study to understand better what it might mean for us; and then there's a very small group where I respectfully have a different view.”

The Director said the report provides an effective roadmap to keeping the FBI a premiere law enforcement and intelligence organization. “I think being world-class means knowing you are good but never being satisfied that you are good enough,” he said. “I believe the FBI is world-class. [The report] shows us ways that we can be better.”

The report's key findings center on the Bureau's transformation since the attacks in 2001. Commissioners focused on elements of how the FBI has adapted over more than a decade, such as the creation of a cadre of skilled intelligence analysts to analyze threats, the retention of good leadership, and the development of cyber capabilities to thwart agile hackers and online threats.

“This has been a major transformation of the FBI in which the intelligence function—which as the Director said has always been there—has been expanded and brought up to date in terms of the

threat in a way which was almost exponential,” said Commissioner Edwin Meese. “Some things are necessary, we feel, that will keep pace with the accelerating threat we find around the world.”

The commissioners issued 12 findings, along with recommendations. Topics include information-sharing, cyber security, technology, the Bureau's legal attaché program, and the FBI's role in countering violent extremism.

“During the decade and a half after 9/11, the FBI has changed,” said Commissioner Roemer. “It is currently changing, but must urgently and boldly accelerate this change. What we've laid out, I hope, is a blueprint for the FBI over the next quarter-century. Over the course of this next century, hundreds of Americans' lives will depend on it.”

Comey said the FBI's progress has been extraordinary and that the Bureau was up to the task. “I think this is a moment of pride for the FBI,” he said. “An outside group of some of our nation's most important leaders and thinkers has stared hard at us and said, ‘You have done a great job at transforming yourself.’ And they've also said what I've said around the country: It's not good enough.”



# FBI Establishes International Corruption Squads

Targeting Foreign Bribery, Kleptocracy Crimes



Late last year, Alstom—a French power and transportation company—pled guilty in U.S. federal court to engaging in a widespread foreign bribery scheme involving tens of millions of dollars. The company agreed to pay a record-setting \$772 million fine to resolve the charges.

Alstom's specific crimes? Violating the U.S. Foreign Corrupt Practices Act (FCPA) for more than a decade by paying bribes to government officials around the world—falsifying its books and records in the process—in connection with power, grid, and transportation projects for state-owned entities.

The FCPA, passed in 1977, makes it illegal for U.S. companies, U.S. persons, and foreign corporations with certain U.S. ties to bribe

foreign officials to obtain or retain business overseas. And we take these crimes very seriously—foreign bribery has the ability to impact U.S. financial markets, economic growth, and national security. It also breaks down the international free market system by promoting anti-competitive behavior and, ultimately, makes consumers pay more.

*We take these crimes very seriously—foreign bribery has the ability to impact U.S. financial markets, economic growth, and national security.*

We're seeing that foreign bribery incidents are increasingly tied to a type of government corruption

known as kleptocracy, which is when foreign officials steal from their own government treasuries at the expense of their citizens. (See sidebar for more on kleptocracy). And that's basically what these foreign officials are doing when they accept bribes in their official capability for personal gain, sometimes using the U.S. banking system to hide and/or launder their criminal proceeds.

The FBI—in conjunction with the Department of Justice's (DOJ) Fraud Section—recently announced another weapon in the battle against foreign bribery and kleptocracy-related criminal activity: the establishment of three dedicated international corruption squads, based in New York City, Los Angeles, and Washington, D.C.

Special Agent George McEachern, who heads up our International Corruption Unit at FBI Headquarters, explains that the squads were created to address the national and international implications of corruption. “The FCPA allows us to target the supply side of corruption—the entities giving the bribes,” he said. “Kleptocracy cases allow us to address the demand side—the corrupt officials and their illicit financial assets. By placing both threats under one squad, we anticipate that an investigation into one of these criminal activities could potentially generate an investigation into the other.”

Corruption cases in general are tough to investigate because much of the actual criminal activity is hidden from view. But international corruption cases are even tougher because the criminal activity

usually takes place outside of the U.S. However, members of these three squads—agents, analysts, and other professional staff—have a great deal of experience investigating white-collar crimes and, in particular, following the money trail in these crimes. And they’ll have at their disposal a number of investigative tools the Bureau uses so successfully in other areas—like financial analysis, court-authorized wiretaps, undercover operations, informants, and sources.

*“The FCPA allows us to target the supply side of corruption—the entities giving the bribes.”*

Partnerships with our overseas law enforcement counterparts—facilitated by our network of legal attaché offices situated strategically

around the world—are an important part of our investigative arsenal. The FBI also takes part in a number of international working groups, including the Foreign Bribery Task Force, to share information with our partners and help strengthen investigative efforts everywhere. And we coordinate with DOJ’s Fraud Section—which criminally prosecutes FCPA violators—and the Securities and Exchange Commission—which uses civil actions to go after U.S. companies engaging in foreign bribery.

Our new squads will help keep the Bureau at the forefront of U.S. and global law enforcement efforts to battle international corruption and kleptocracy.

### **Kleptocracy 101**

*Last year, the Department of Justice announced it had forfeited more than \$480 million in corruption proceeds hidden in bank accounts around the world by former Nigerian dictator Sani Abacha and his associates. It was the largest forfeiture ever obtained through a kleptocracy action.*

*And earlier this month, DOJ announced a settlement of its civil forfeiture cases against \$1.2 million in assets traceable to corruption proceeds from Chun Doo Hwan, former president of the Republic of Korea. DOJ also assisted in recovering an additional \$27.5 million to satisfy an outstanding criminal restitution order against the former president.*

A kleptocracy—loosely translated from Greek as “rule by thieves”—is

a form of political or government corruption involving officials who steal from their government treasuries to enrich their own personal wealth.

Both previously mentioned cases were opened under DOJ’s Kleptocracy Asset Recovery Initiative, which—in coordination with the FBI and other federal agencies—seeks to forfeit the proceeds of corruption by foreign officials and, where appropriate, use the recovered assets to benefit the people harmed by the acts of corruption. Both cases, investigated by the FBI, are prime examples of kleptocracy-related criminal activity: Through bribes and other schemes, these “kleptocrats” stole money from their own governments and used the U.S. banking system, among others, to launder the funds.

In addition to impacting the U.S.

economic sector, kleptocracy and international corruption have national security implications. According to Special Agent Jeffrey Sallet, chief of the FBI’s Public Corruption/Civil Rights Section, “Corruption leads to lack of confidence in government. Lack of confidence in government leads to failed states. And failed states lead to terror and national security issues.”

How does the FBI get its kleptocracy cases? We may open cases on the same foreign officials we identify in our Foreign Corrupt Practices Act investigations. In addition, our foreign law enforcement partners and/or new leaders in certain parts of the world often seek U.S. assistance in identifying and recovering government assets stolen by previous corrupt regimes.



# National Explosives Task Force

## A Multi-Agency Group of Bomb Experts

Bomb threats are not a new tactic for criminals and terrorists, but when scammers used them in a ruse in 2013 to fraudulently obtain pre-paid money cards from retailers around the country, first responders needed to know about it. A bulletin was sent to public safety officials explaining the scheme. The notice advised that although no devices had been found linked to this particular threat, first responders should not automatically assume any bomb threat is a hoax.

The awareness bulletin was a product of the National Explosives Task Force (NETF), a multi-agency assemblage of bomb technicians, analysts, and professional staff that formed in 2011 to quickly analyze and disseminate intelligence related to improvised explosive devices (IEDs) and other explosive materials in the U.S. The task force, located at FBI Headquarters, includes personnel from the FBI, ATF, DHS, and the Office of the Director of National Intelligence. The arrangement puts some of the nation's leading bomb experts together in the same room.

"We are trying to create a common operating picture for the government to see what the problem set is domestically in terms of explosives and IED incidents," said Whitney Barnhart, an FBI analyst who has been on the task force since its inception. "And we're using that information to create products to support federal, state, and local bomb technicians and the work that they're doing."

The NETF's main functions include gathering and analyzing intelligence on explosives, integrating the intel into investigations, and pushing information out to partners—

which include more than 3,100 public safety bomb technicians on more than 400 bomb squads around the country. The task force is notified every time the FBI or the ATF responds to an explosives-related incident and also reviews explosive incidents reported by public safety bomb squads, military explosive ordnance disposal teams, and other reporting sources.

"It became apparent years ago that we needed an interagency task force looking at the intelligence from these IED incidents and quickly pulling together joint intelligence products for the bomb tech community to make sure that everybody is situationally aware," said James Yacone, assistant director of the FBI's Critical Incident Response Group, under which NETF operates.

Depending on circumstances, the task force might push out a detailed "Quick Look" report (within 24 hours of a major incident), an industry advisory, or an awareness bulletin like the bomb threat scam advisory in 2013. The bulletins typically contain device information and tactics, techniques, and procedures used by the perpetrator(s) to raise awareness among people who most need to know. Last May, for example, the task force sent an industry advisory about the use of chemical reaction bombs after four similar incidents occurred in the Washington, D.C. area. (Fortunately, the perpetrators in these incidents were quickly arrested.) And last October, an advisory sought to bring attention to the dangers of unexploded munitions at recycling facilities after an explosion at one in Illinois killed two employees.

"We're taking information that's



**One role of the National Explosives Task Force is to alert partners to potential incidents through the use of bulletins and advisories, such as the one above regarding unexploded munitions at recycling facilities.**

coming in to be more proactive about what we're seeing ahead of events and incidents," said Barnhart, the NETF analyst.

Another example is a system the task force developed to notify key personnel in local jurisdictions when inmates held on explosives-related charges are set to be released in their areas. The Bureau of Prisons notifies the task force, which vets the information and distributes it to ATF field offices and FBI bomb techs. Bradley Cooper, an ATF analyst who helped develop the inmate-release notification with an FBI partner, said the multi-agency approach makes sense.

"When everybody comes together from different agencies to work a common goal, it's remarkable," said Cooper, whose task force experience includes working alongside FBI personnel after the 1995 Oklahoma City bombing.

The full weight of the task force's effectiveness comes into focus when a major event occurs. When multiple agencies gather in a command post, they know each other and they know who has the critical explosives expertise to work an investigation.

"That's the beauty of NETF," Yacone said. "It brings together all the special mission experts."

# Public Corruption

## FBI Agent Helps Protect His Native American Community

When Special Agent Jeff Youngblood helped convict a corrupt public official from the Choctaw Nation of Oklahoma last year who was demanding bribes and kickbacks from contractors bidding on tribal construction projects, he felt more satisfaction than usual bringing a criminal to justice. That's because Youngblood is Native American and a member of the Choctaw tribe.

"My dad was born and raised in this area, and Oklahoma is where I was born and raised," said Youngblood, who is assigned to the FBI's Oklahoma City Division and works in the southeastern part of the state that is home to the Choctaw Nation.

"There aren't many Native Americans who are special agents," he said, "and I have yet to meet any that are working in Indian Country and are enrolled members of the tribe where they work. I think mine is a unique situation."

It's a situation Youngblood embraces. The Durant Resident Agency, where he is stationed with one other agent, has responsibility for a six-county area that covers much of the Choctaw Nation. With a large casino resort complex in Durant—located only an hour's drive from Dallas, Texas—the tribe is a major economic driver in the region, and many residents depend on it for their livelihood.

When Youngblood received a tip regarding improprieties by the executive director of construction for the tribe, he began to investigate. He soon discovered that Jason Merida was running a classic "pay to play" system, shaking

down contractors for cash, trips, vehicles, guns, and other items in return for lucrative construction projects.

"If he didn't get what he wanted, you weren't going to get the job," Youngblood said. Some of the contractors who paid bribes to win contracts then padded their invoices, Youngblood noted, "which cost the tribe additional money."

Merida was indicted in February 2014 and charged with conspiracy to commit theft or bribery from programs receiving federal funds, theft by an employee or officer of a tribal government receiving federal funds, money laundering, and tax fraud.

Testimony at trial in November 2014 revealed that Merida and others submitted and approved false invoices from subcontractors, allowing Merida to steal more than \$500,000 in funds from the Choctaw Nation. He was found guilty on a variety of theft charges and is currently awaiting sentencing.

"Through interviews, analysis of bank records, and other investigative techniques, we were able to identify a lot of assets that were fraudulently given to Merida," Youngblood said. "There was an excessive waste of the tribe's money because of a few people's greed." And as the investigation went on, Youngblood realized that he, too, was a victim.

"I understood what all that money could have been used for—maybe to help with my children's education or the educational needs of other members' children or many other worthy tribal causes," he said.



**FBI Agent Jeff Youngblood works Indian Country matters in Oklahoma—including cases involving the Choctaw Nation, of which he is an enrolled member.**

"So much good could have been done with that money."

He added that "a lot of honest companies got squeezed out" because they didn't pay to play, "and those companies' employees have families that live here in Southeastern Oklahoma, and they were robbed of an opportunity to have gainful employment because of these individuals."

Youngblood believes this investigation should send a message—"not only here in the Choctaw Nation but for all the tribes in the region: If you're going to do work for the Indians, it better be honest and done fairly. If not, we will find you and we will prosecute you."



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/pcindiancountry](http://www.fbi.gov/pcindiancountry).



# Violent Gangs

## Kidnapping Crew Targeted Criminal Community



The Dominican street gang in Lawrence, Massachusetts must have thought they had the perfect illegal enterprise: kidnap drug dealers, bookmakers, and money launderers, steal their cash and drugs, and then hold them for ransom—knowing that since the victims were themselves criminals, they and their families would likely never report the abductions.

The gang members—known as joloperros, or stick-up guys—were organized, armed, and violent: They often tortured their victims, sometimes with hot irons.

“They targeted anyone they thought they could make large sums of money from,” said Special Agent Jeff Wood, coordinator of the North Shore Gang Task Force, one of the FBI’s three Safe Streets Task Forces in Massachusetts.

The kidnappings began around 2010 in and around Lawrence, a largely Hispanic city and gang stronghold located about 20 miles north of Boston. The North Shore Gang Task Force—made up of the FBI, the Massachusetts State Police, the Lawrence Police Department, the Massachusetts Department of Corrections, and

other local law enforcement agencies—worked with the Drug Enforcement Agency to build a case against the crew.

“The victims and their families would not report the crimes,” Wood said, “because they didn’t want to admit that, yes, they were selling drugs or laundering money. And some of the victims were in the country illegally.”

The joloperros mainly targeted drug dealers, and their methods were sophisticated. They used GPS devices to track individuals, conducted surveillance to learn targets’ routes and movements, and also tried to identify dealers’ stash houses

***“They targeted anyone they thought they could make large sums of money from.”***

“They weren’t targeting street-level dealers, but rather suppliers,” Wood said. Some of the victims were selling multiple kilos of heroin and cocaine on a monthly basis.

When the actual abductions took place, the crew would grab the victim, duct tape his hands, and

put a cover over his head. Victims were taken to safe houses, where they were often tortured, and large ransoms were demanded from their families.

“When we got word of a kidnapping, we would go to the family and they wouldn’t cooperate,” Wood said. But over time, using a variety of investigative techniques such as confidential sources, controlled drug buys, and other means, most of the crew was dismantled.

Last month, after previously pleading guilty to a violent 2012 kidnapping in which a \$100,000 ransom was demanded, Edgar Acevedo was sentenced to 16 years in prison.

Since the task force investigation began more than two years ago, approximately 20 individuals have been charged in federal court—including some of the gang’s leaders—with kidnapping-related offenses or for crimes associated with the Lawrence-based kidnapping crews. To date, nine people have pled guilty to conspiracy to commit kidnapping, and four others have pled guilty to firearm-related offenses. Several joloperros are awaiting trial.

“At one point, these kidnapping crews had a very large presence in Lawrence,” Wood said, “but their presence has decreased dramatically thanks to law enforcement intervention.” He noted that many people associate violent gangs with Los Angeles or the Southwest Border, “but gangs are just as violent and just as dangerous in upstate Maine as they are in Los Angeles. They lower the quality of life in the community they are operating in, no matter where that community is.”



# The Oklahoma City Bombing

20 Years Later



## The Oklahoma City Bombing 20 Years Later

*This article is a special extended feature commemorating the 20th anniversary of the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City.*

As Oklahoma City and the country prepare to mark the 20th anniversary of the Alfred P. Murrah Federal Building bombing on April 19, 1995, FBI.gov looks back at the deadliest act of homegrown

terrorism in the nation's history through the eyes of special agents who were there and a survivor who continues to honor the victims by sharing her remarkable story.

The Ryder truck packed with nearly 5,000 pounds of explosives that Timothy McVeigh parked in front of the Murrah building that Wednesday morning killed 168 people, among them 19 children—most of whom were in the building's daycare center. The youngest victim was 4 months old. Hundreds of all ages were injured.

In a matter of seconds, the blast destroyed most of the nine-story concrete and granite building, and the surrounding area looked like a war zone. Dozens of cars were incinerated, and more than 300

nearby buildings were damaged or destroyed. Immediately, the FBI turned its full attention to Oklahoma City. The OKBOMB investigation, as it became known, remains one of the largest and most complex cases the FBI has ever undertaken.

### *'I Never Thought it Was a Gas Explosion'*

When the bomb went off, Special Agent Jim Norman was at his desk at the FBI's Oklahoma City Field Office, located about five miles northwest of the Murrah building. "It shook everything in the office," Norman recalled. "Files fell off people's desks where they were piled up." One of the Bureau's senior bomb technicians, Norman, now retired, rushed into his supervisor's office. "We looked toward downtown Oklahoma City and you could see a tan cloud of debris rising from that area. I told my supervisor, 'I think a bomb detonated downtown. We need to go down there.'"



**Left: The bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995 was the deadliest act of homegrown terrorism in U.S. history, resulting in the deaths of 168 people. In a matter of seconds, the blast destroyed most of the nine-story building, incinerated nearby vehicles, and damaged or destroyed more than 300 other buildings.**



In his car on the way to the scene, a local radio station was reporting that the blast might have been caused by a natural gas explosion, but in his gut, Norman knew it was a bomb from the sound he had heard. “I never thought it was a gas explosion,” he said. Less than 15 minutes after the blast, he parked two blocks away from the Murrah building. It was as close as he could get because of all the debris.

“I ran over to where all the smoke was,” he said. “As I was heading that way, a number of people were running in the opposite direction. I approached the north entrance and couldn’t believe what I was seeing. The whole front of the building had been torn off. On the left side of the building, in some places the flooring had been torn away all the way to the back wall. That building was 200 feet wide and 80 feet deep.”



Special Agent Jim Norman (seated, left) was one of the first FBI agents to arrive at the Murrah building after the explosion. He was appointed to supervise the OKBOMB investigation.

Standing before the massive, tangled pit of debris and bodies, Norman began thinking like the seasoned bomb tech and investigator that he was. And a thought occurred to him: “Our lives have changed forever,—because I knew the magnitude of what we were facing.”



Florence Rogers was head of the Federal Employees Credit Union. When the bomb went off, she was in her third-floor office at the Murrah building holding a meeting with eight of her employees. She was the only one in her office who survived. (AP Photo)

### *‘Where Are You Guys?’*

Florence Rogers, head of the Federal Employees Credit Union, was in her office on the third floor of the Murrah building that morning. Seated around her desk were eight credit union employees, some of whom Rogers had known and worked with for decades. Although they were having a business meeting, spring was in the air, and there was talk of the women’s colorful seasonal dresses.

When the bomb went off at 9:02, Rogers was thrown backward onto the floor, her desk and other office items landing all around her. When she looked up, every one of her colleagues had vanished. “I started hollering, ‘Where are you guys? Where are you guys?’”

In the next moments, before building and car alarms triggered by the blast began to howl, before fire engine and police sirens wailed, and before cries rang out from the trapped and injured, Rogers

experienced an “eerie silence.” Alone on a narrow ledge—all that was left of her office floor—below which was a deadly, open pit, she wondered where her colleagues had gone. She wondered why she could see daylight where walls and ceilings should have been. And later, after being helped to safety, she would wonder at the miracle of her own survival on a day when so many had perished.

### *‘You Immediately Snapped Your Head Toward Town’*

Special Agent Barry Black was at Tinker Air Force Base that morning tracking a fugitive in a stock manipulation case he had been working on for four years. Black was trained as an accountant, but since joining the Bureau seven years earlier, he had become a sniper on the SWAT team and had deployed to the Waco standoff in 1993—the event that had galvanized Timothy McVeigh’s hatred of the federal government. Black was also the newest bomb tech in the Oklahoma City Division.



Special Agent Barry Black in 1995.



Left: Barry Black, Special Agent, Oklahoma City FBI

## Misguided Revolutionary

Timothy McVeigh targeted the Murrah building largely because it was full of U.S. government workers like Barry Black's wife. Fourteen federal agencies had offices there, and 98 of the victims worked for the federal government.

McVeigh, a decorated Army veteran, believed the government was attacking Americans' personal rights and freedoms. His anger hardened on April 19, 1993, when 76 men, women, and children died in a fire during an armed standoff with federal agents in Waco, Texas. Many mistakenly believed that federal officers had set the fire. McVeigh, who visited Waco during the standoff, said that the government had declared war against the American people. He planned to fire the first shot in a new American revolution.



Timothy McVeigh's hatred of the federal government intensified in 1993 after an armed standoff in Waco, Texas resulted in the deaths of 76 people. McVeigh went to Waco during the standoff and handed out anti-government literature.

He and his partner had received a tip that their white-collar fugitive was on the military base, and as they waited in their car for him, the bomb went off.

They were seven linear miles from the Murrah building. "I remember it was very loud and you immediately snapped your head toward town," he said. "It was loud enough where you could see the people outside hunker down because of the noise." It was later determined that the blast registered 3.2 on the Richter scale—very much like an earthquake.



Members of the OKBOMB Task Force were issued special credentials.

"There was a big cloud of smoke already blowing to the north," Black said. "We had no idea what had happened," but they knew it was a major event. "So the emergency part took precedence over a white-collar crime," he explained, and they quickly returned to the office. The fugitive's arrest would have to wait until another day.

After a discussion with his supervisors, Black, who is currently approaching his 27th year with the Bureau, drove to the blast site to help determine what had happened. When he saw the destruction at the Murrah building, there was an even greater urgency to his mission, because his wife, Kelly, was a federal employee who worked there. In the days before most people had cell phones, he said, "I wasn't sure where she was."

About 90 minutes later, Black's wife was able to leave a message on his pager that she was safe. She and two colleagues had emerged from the Murrah building garage at 9 o'clock and had driven in front of the Ryder truck on their way to the highway. Black understood that had his wife been delayed by a mere two minutes, she never would have survived.



## *'Jump In and Work as Hard as You Could'*

Bob Ricks was the special agent in charge of the FBI's Oklahoma City Division in 1995. On the morning of April 19, he and many of his law enforcement colleagues were signed up for a charity golf event about 40 miles east of downtown sponsored by the Oklahoma State Bureau of Investigation. His counterparts from the Secret Service and U.S. Marshals Service were there as well.

"We were just getting ready to tee off, and all of a sudden everyone's phones started going off. I got a call from my secretary saying that there had been some type of a bombing down at the Murrah Federal Building—didn't know how bad it was."

Ricks, currently chief of the police department in Edmond, a town just outside Oklahoma City, had a long career with the Bureau and



**Bob Ricks, Former Special Agent in Charge, Oklahoma City**

had previously helped establish a Joint Terrorism Task Force in New Jersey. He understood bombing incidents, and they usually turned out to be small pipe bombs that did minor damage. In his experience, most individuals who carried out such attacks were trying to make a statement, not kill anyone.

Ricks got back to Oklahoma City in a hurry and remembers one of his assistants asking him, "Bob,

you know what today is?' At first I didn't know what he was talking about. And he said, 'Today is April 19,' which was the last day of the standoff at Waco. That immediately set off an antenna that we probably had a reprisal that had taken place as a result of the Waco situation."

With the bomb squad and other resources already dispatched to the scene, Ricks set about standing up a command post. There was never a question that the FBI would take charge of the case.

"My first job was to get together with the leadership of the fire department and the police department and make sure we had a unified command," Ricks said. He arranged a meeting with the chiefs of the Oklahoma City police and fire departments outside what was left of the Murrah building, which looked as if it might topple at any moment.



**Bob Ricks (left) was the special agent in charge of the Oklahoma City Field Office in 1995. Former FBI Director Louis J. Freeh (right) visited Oklahoma City after the bombing.**



Within hours of the bombing, the FBI established a command center a few blocks from the Murrah building to coordinate recovery and investigative efforts and to integrate the local, state, and federal agencies that were assisting. “The first day or so, it really was chaotic,” said Bob Ricks, then special agent in charge of the FBI’s Oklahoma City Division. “What you are trying to do is bring some sense of order to the chaos.”

After the meeting, he recalled, “We all went back to doing what we were doing, and I kind of stood there in front of that building by myself for a while, and all I could do is think to myself, ‘Lord this was overwhelming, and where do you start?’ And I basically said a prayer. ‘Obviously I can’t make it right, but hopefully we can find justice in this process.’”

By mid-afternoon, a telephone company provided space near the blast site for a command center, complete with 190 phone lines. The investigation was in full swing. FBI photographers took pictures, bomb techs looked for secondary explosives, SWAT provided security, evidence technicians fanned out looking for evidence, and agents interviewed witnesses and began to track down information and send leads to other FBI offices. At FBI Headquarters in Washington, officials began diverting resources to help the 120 special agents based in Oklahoma City.

At the command center, Ricks said, “The first day or so, it really was chaotic. What you are trying to do is bring some sense of order to the chaos. We started immediately trying to

work together.” The command center essentially became another FBI field office. “From the basic infrastructure of getting telephones together, of trying to get together a records management system, of coordinating with the fire department to get our evidence response teams on the ground, to seal off the inner perimeter, to have an outer perimeter, to have control of the press as to how we were going to handle messaging. And so you really start from the ground up. Building this infrastructure, that was necessary, and at the same time integrating all of these different agencies—local police, local fire, local sheriffs, federal agencies—into this process.”

“I think we all understood the enormity of what it was,” he added. “To keep your sanity, the best thing you could do was jump in and work as hard as you could to try to get this thing solved.”

### *The Path to McVeigh*

Evidence quickly led to Timothy McVeigh. Investigators determined the explosion was caused by a truck bomb and collected vehicle parts with telltale bomb damage. A vehicle identification number led to

a Ryder rental facility in Junction City, Kansas. On April 20, the FBI released a sketch of the man who rented the truck. The owner of the Dreamland Motel in Junction City recognized him as a guest registered as Timothy McVeigh.



A day after the bombing, the FBI released a sketch of a suspect who rented a Ryder truck in Kansas. That suspect was Timothy McVeigh.

A search of police records showed that McVeigh was in the Noble County jail in Perry, Oklahoma. A state trooper had stopped him shortly after the bombing because his car was missing a license plate. He arrested McVeigh for carrying a concealed firearm, and McVeigh was still in custody when the FBI called.

McVeigh used a Michigan address when he checked into the Dreamland Motel. He listed the same address—which belonged to a brother of Terry Nichols—when





Timothy McVeigh was arrested 90 minutes after the bombing when an alert trooper noticed that his vehicle (left) did not have a license plate. The axle from the truck bomb (center) contained an identifying number (center, inset) that was traced back to the Ryder truck McVeigh rented in Kansas. Special Agent Barry Black (right) inspects parts of the Ryder truck that were collected as evidence, which are now archived at the Oklahoma City National Memorial & Museum.

he was arrested shortly after the bombing. Terry Nichols was one of McVeigh's Army buddies also known for his anti-government sentiments, and the investigation showed that Nichols helped McVeigh buy and steal the material for the bomb and helped mix the ingredients.

Before the bombing, McVeigh spent time in Arizona with Michael Fortier, another Army friend, where he shared his plans and described how he would place the barrels of explosives in the truck. To help finance the plot, Fortier sold guns that McVeigh and Nichols had stolen.

Investigators discovered plenty of other evidence. The clothes McVeigh was wearing when he was arrested—along with a set of earplugs in his pocket—tested positive for chemical residue used in the explosive. Jim Norman said of McVeigh's clothes: "When we sent that clothing back to the FBI Laboratory and they did a chemical analysis test, they determined that he was basically the explosive equivalent of a powdered sugar donut."

McVeigh's fingerprints were also found on a receipt at Nichols' home

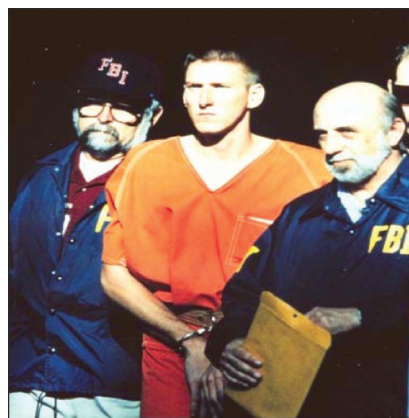
for 2,000 pounds of fertilizer used to make the bomb. Other evidence linked McVeigh and Nichols to each other and to different elements of the crime.

### *No Stone Unturned*

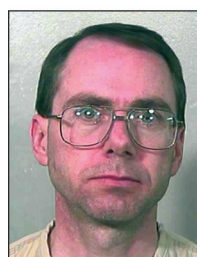
While the OKBOMB investigation quickly turned to McVeigh, Nichols, and Fortier, the FBI initially had no idea how many people were involved. In 32 months, the Bureau logged more than 1 million hours of investigative work through the OKBOMB Task Force. During that time, investigators conducted more than 28,000 interviews, followed more than 43,450 investigative leads, collected nearly 3.5 tons of evidence, searched 1 billion records in 26 databases, and reviewed more than 13.2 million hotel registration records, 3.1 million Ryder truck rental records, and 682,000 airline reservation records.

In August 1995, McVeigh and Nichols were charged with the same 11 federal crimes:

- Conspiring to use a weapon of mass destruction to kill people and destroy federal property;



Flanked by FBI agents—including Jim Norman, left—Timothy McVeigh is taken into federal custody.



Terry Nichols



Michael Fortier

- Using a weapon of mass destruction that caused death and injury;
- The malicious destruction of federal property by explosives; and
- Eight counts of first-degree murder of federal law enforcement officers.

A federal jury found McVeigh guilty of all counts on June 2, 1997. He was executed on June 11, 2001. A different jury found Nichols guilty of conspiracy and eight counts of manslaughter on December 23, 1997. He was sentenced to life in prison. Fortier testified against McVeigh and was sentenced to 12 years in prison for failing to report the planned attack and for lying to the FBI.

### *'The System Worked as it Should'*

**"T**he whole event was absolutely senseless," Barry Black said. "I



Special Agent Barry Black is nearing his 27th year with the FBI.



Bob Ricks is currently the chief of police in Edmond, Oklahoma.



Retired Special Agent Jim Norman was the lead investigator for OKBOMB.

have given a lot of presentations at various schools and universities, and depending on the age of the folks, they always want to know, 'Why did it happen?' or, 'Why did it happen here?' If the goal was to overthrow the government or change the government, well, in our country you do that every four years—peacefully. Power changes hands. This didn't work out as McVeigh and Nichols had hoped it would."

Black is satisfied with the soundness of the American judicial system. "I'm proud that the system worked as it should," he said. "The subjects were caught, the evidence was collected and presented. The jury heard it and made its decision, and the law was carried out. So regardless of the scale and size of an event, it can be addressed and handled appropriately."

In the end, despite the evil that some individuals are capable of, Black believes "good folks tend to prevail."

Bob Ricks, too, is proud of the OKBOMB investigation. "I think it's one of the finest hours in the history of the FBI," he said,

adding, "If you talk to those in the community around here, the FBI probably has one of the best relationships with any city in the country. Part of that is us all working together on the bombing and feeling a sense of accomplishment that we were able to put this all together in a very successful fashion."

Jim Norman, one of the first FBI agents to arrive at the Murrah building after the explosion, was assigned as the lead investigator for OKBOMB. "I am very proud of the work that everybody did," he said. "We had all these people that came together, and they did the very best they could." He added that the bombing still represents a defining moment for Oklahoma citizens. "When you try to talk about something that happened, that was before the bombing or that was after the bombing. It's a measure of time like BC and AD."

The current FBI special agent in charge in Oklahoma City, James Finch, agrees. "One of the things you become acutely aware of," he said, "is that you can talk to a small child or a very elderly person



James Finch, Special Agent in Charge, Oklahoma City FBI



in Oklahoma, and what you will find, even though their way of expressing it will be vastly different, is they will have an awareness of the bombing. If it's a child and they weren't born at that time, it's almost like it was passed on." Through school programs and visits to the museum and memorial site, he explained, "They know it's a part of their existence as Oklahomans."

Finch, originally from Nebraska but who now calls Oklahoma home, pointed out the resiliency of residents who responded to the bombing with a can-do attitude and heartfelt appreciation and support for all those who came from out of town to help. That collective good will became known as the Oklahoma Standard.

### *'Enormous Generosity and Kindness'*

Dr. William Fabbri is a medical doctor and the director of the operational medicine program at the FBI. At the time of the bombing, he was not an FBI employee. He was an emergency medical physician working in a trauma center in Baltimore, Maryland, and he was

also a member of the urban search and rescue program administered by the Federal Emergency Management Agency. Fabbri and other doctors teamed with firefighters to form collapse rescue teams.

Although the team's primary mission was to aid with natural disasters, not man made ones, they were called to Oklahoma City after the bombing. "I don't think any of us ever thought we'd be involved with a crime scene or an incident of this magnitude," Fabbri said. But 46 hours after the explosion, he got a firsthand look at the devastation wrought by domestic terrorism.

"It was an awful, horrific event," he said, "but the response of the people of Oklahoma and Oklahoma City was absolutely phenomenal." Fabbri's experience, like those of so many first responders, speaks volumes about the Oklahoma Standard.

"On the first day of working, all of sudden we have civilians being escorted in by law enforcement, offering food, and we have representatives from the cellular companies handing us these big, brick-like cell phones that you had

back in '95—because not everyone had one in those days—and saying, 'Use these for whatever you need them for, and we will be by periodically to change out the batteries.'"

After his first 12-hour shift inside the Murrah building, Fabbri joined many of the responders who were walking back to where they were staying. "What started to happen over a period of the first few days," he said, "is that when we exited the security cordon, there were people waiting to greet us, talk with us, and thank us. And the longer we were there, the more of that there was."

The first responders and investigators learned they could always count on residents preparing food for them—available at any time of day or night, since work went on at the site around the clock.

"After a few days," Fabbri said, "you learned to be very careful about comments in public about things that you didn't have." A dog handler, for example, was approached by a local resident who casually asked what kind of food the dog ate. "Within a very short time, the command post called and said, 'There are 40 bags of dog food here for your team.'"

One night waiting in line for dinner, Fabbri commented that he should have brought a pair of sneakers with him—he had only packed two pairs of work boots. A few hours later, "someone was walking around trying to find the firefighter who needed sneakers. Someone had gone to a shoe store and showed up with a bunch of sizes, and it was really remarkable. The people were so gracious and willing to help."



Dr. William Fabbri, Director of Operational Medicine, FBI



Cathy Keating, wife of Oklahoma's then Governor Frank Keating, visited with investigators and first responders to thank them for their efforts after the bombing. The outpouring of support and generosity shown to law enforcement and responders from residents became known as the Oklahoma Standard.

That fact was all the more amazing considering that the majority of Oklahoma City residents were either victims of the bombing or had friends or family who were victims. "It was a fascinating duality between this enormous generosity and kindness of the people and this tremendous sadness and pain that they were going through," Fabbri said, "and the two were connected. Partly as the result of that, a bond developed between the rescuers and the people of

Oklahoma City that I suspect still exists to this day."

Until the bombing, Fabbri had never considered a career with the FBI. Three years later, he joined the Bureau. "My first day," he recalled, "my wife gave me a photograph of what is now called the Survivor Tree, which is immediately across the street from the north side of where the Murrah building stood. If you look at video from that time, there is a

whole parking lot full of cars that are on fire, and the tree is actually in that parking lot. It was a surprise to the locals that the tree wasn't destroyed, and it became a sort of talisman. The day I started working here, my wife gave me a framed picture of the tree with a quotation that basically says that experiences like this tend to concentrate the mind on every good thing. And it's on the wall right next to my desk."





A collapse rescue team from Maryland was one of many teams from around the country to offer assistance after the bombing.



Immediately after the explosion, FBI personnel were dispatched to the Murrah building to begin the painstaking process of collecting evidence, even as firemen and other first responders worked to recover victims and stabilize the area.



## *'It's About Remembering'*

Today, on the site of what was once the Murrah building, there is a fitting memorial and museum honoring the significance of that tragic day.

"The memorial is really built to remember those who were killed and those who survived and those who were changed forever," said Kari Watkins, executive director of the Oklahoma City National Memorial & Museum. "One of our missions was to build a place that would teach the moral of the story and the tenderness of the response."



Kari Watkins, Executive Director, Oklahoma City National Memorial



The Oklahoma City National Memorial & Museum was dedicated on April 19, 2000, five years to the day after the bombing. "The memorial is really built to remember those who were killed and those who survived and those who were changed forever," said Executive Director Kari Watkins. Two towers on either side of a reflecting pool where the Murrah building stood show the time immediately before and after the explosion. In the museum, visitors can see a room of twisted metal and concrete fragments left untouched after the bombing, along with a variety of interactive exhibits. In the memorial area, there is a chair for each of the 168 victims. Between the memorial and museum stands the Survivor Tree, which survived the blast and subsequent fires and symbolizes the notion that good will always triumph over evil.





Survivor Florence Rogers believes she has a responsibility to bear witness to the tragedy so that no one will forget it.

“A building was attacked to try to defeat the government,” she explained, “and what happened was a unity like none we have seen. People came together and worked together and said, ‘The government will survive.’ And after two days, the federal credit union reopened and federal agencies reopened, and that’s a part of the story that we want to retell: Even though people try to bring down the very government we believe in, we will survive, and it will be that same government that will defend the criminals and prosecute the criminals at the same time. And that’s a pretty remarkable story.”

Watkins added that the museum and memorial teach each new generation about the bombing and the response to it so that future generations are less likely to repeat the same mistakes. “This place is as relevant today as it was 20 years ago,” she said. “It’s about remembering.”

### *‘The Whole World was Touched’*

Perhaps as much as anyone, Florence Rogers symbolizes the need—and the duty—to remember.

The former head of the credit union, who survived while the eight women in her office only a few feet away were killed, embodies the strength, spirit, and good will that give life to the concept of the Oklahoma Standard.

She tells her story as way to honor the dead and to ensure that people will remember the good that came from the bombing as well as the tragedy. “The whole world was touched by what happened in Oklahoma,” she said.

“I had 32 full-time employees. I lost 18 of those 32; several of the others were seriously injured. Those 18 that I lost had worked for me 128 years total tenure. They were like my daughters, some of them,” she said. “It hurts

to see their families, and here I am having great-grandbabies, and those families won’t ever have that opportunity. I soothe myself, I guess you’d say, by saying that God was not ready for me that day.”

“There’s not a day goes by that I’m not reminded of it,” Rogers said of the bombing, but remembering and telling her story is a way to give back to the community, “and I find a lot of healing in doing that.” She added that it’s “rewarding to see the family members. I remember when I got a call from one of the mothers who had lost her daughter, and she said, ‘Florence, I’m so glad that you made it out of there.’ And I started sobbing, because she gave it all, and she was glad that I had made it out.”

One of the most important lessons Rogers learned, she said, “is how short life can be. My advice is, don’t ever miss an opportunity to tell those that you love that you love them, because you never know when you might not come home from that ordinary day.”

# Justice for Victims

## Restitution Ordered in Decade-Long Ponzi Scheme

For more than decade, up until February 2014, Sacramento businessman (and Ponzi scammer extraordinaire) Deepal Wannakuwatte fooled his investors and his lenders into believing that he and his companies were worthy of their trust and their money. During that time frame, he fraudulently obtained in excess of \$230 million from more than 150 victims, including individuals, businesses, government agencies, and financial institutions. Wannakuwatte used this to fund other business ventures, make adequate payments to his investors and lenders to keep the scam going, and line his own pockets.

But on the heels of a joint investigation with the Internal Revenue Service-Criminal Investigation (IRS-CI) and the Department of Veterans Affairs Office of Inspector General (VA-OIG), Wannakuwatte—who pled guilty last year—got his comeuppance: He was ordered by a federal judge last month to pay millions in restitution to his victims. And he'll be doing that from his jail cell, where he'll be serving out his 20-year sentence.

The case began in September 2013, when our Sacramento office was contacted by a representative of one of Wannakuwatte's business associates who thought he might be the victim of a Ponzi scheme. The FBI joined forces with IRS and VA investigators and began looking at Wannakuwatte, his businesses, and his financials.

And after several months of reviewing more than 10 years' worth of business records, analyzing tax and other financial documents, conducting interviews of employees and victims, serving search warrants, etc., law enforcement

was able to piece together how the scam worked.

Wannakuwatte told his victims that his Sacramento-based companies—International Manufacturing Group (IMG) and Relyaid Global Health Care—were involved in the international manufacture and sale of latex gloves. He falsely claimed that his companies did tens of millions of dollars in business with federal agencies every year, most notably the Department of Veterans Affairs.

### *The impact on the victims in this case was often devastating.*

As an aside, IMG actually had been in business for more than 25 years and actually did sell gloves and other supplies to businesses, including medical providers. And he did have a contract with the VA, but it was only for up to \$25,000 a year. The legitimate part of IMG had been losing money for years, and Wannakuwatte used some of the proceeds of his Ponzi scheme to keep the company afloat.

Wannakuwatte offered his investors several different bogus high-yield investment opportunities, most of which related to his purported relationship with the VA. And to prove his bona fides to potential investors and to lenders he was trying to borrow money from, he showed them phony corporate documents as well as actual personal and corporate tax returns where he had reported and paid taxes that falsely overstated his personal income and annual gross receipts and sales for IMG.

At times, Wannakuwatte set up fake conference calls between



himself, a potential investor, and someone he falsely claimed was a VA representative. The purpose of these calls was to convince investors that he really did have a significant business relationship with the VA and that their money would be safe with him.

Unfortunately, it wasn't. And while Wannakuwatte made payments to some of the earlier investors as a way of pacifying them, eventually the scam began to implode as more investors and lenders wanted what was owed them and Wannakuwatte couldn't make the payments.

The impact on the victims in this case was often devastating. For individual investors, Wannakuwatte had encouraged them to obtain their investment money from the equity in their homes or from their retirement accounts—as a result, many lost everything. Losses incurred by the victim financial institutions often threatened their financial stability and reputations. And while his victims suffered, Wannakuwatte purchased luxury homes, vehicles, airplanes, and even a professional tennis team.

The lesson learned from a case like this? Do your due diligence when thinking about investing your hard-earned money.



# Death Notification with Compassion

## FBI Teams Up with Penn State to Offer Online Training

At an event held last week at FBI Headquarters, the Bureau—in conjunction with its partners at Penn State University (PSU)—announced a new, no-cost training website for law enforcement agencies and other first responders responsible for notifying the family members of those who have died suddenly as a result of a crime, an accident, a suicide, or other type of incident.

This initiative was developed to better equip law enforcement personnel, victim advocates, coroners, medical examiners, chaplains, hospital staff, and others who find themselves delivering death notifications to do so with professionalism, dignity, and compassion. Not only because it's the right thing to do, but also because the way a death notification is made can have a significant impact on a family's grieving process and on potential future prosecutions. Director James Comey, who spoke at the event held during National Crime Victims' Rights Week, said, "We have to be better when we intersect with people at the most painful moment in their entire lives."

The training is entitled "We Regret to Inform You..." and can be accessed at [www.deathnotification.psu.edu](http://www.deathnotification.psu.edu).

Funded under the FBI's Active Shooter Initiative, the 45 minute online learning module—available to first responders nationally and internationally—begins with an impact video featuring Karen Schmoyer, the mother of a Pennsylvania murder victim, who shares her personal experiences of when and how she was told of her 15-year-old daughter's death. The training also features descriptions of a proper four-step death



A scene from the demonstration video embedded in the "We Regret to Inform You..." online training module developed jointly by the FBI and Pennsylvania State University to provide assistance to law enforcement and other first responders charged with providing death notifications to victims' next of kin.

notification process that includes extensive planning and preparation for the visit to the next of kin, the actual visit to deliver the notification, and the follow-up with the family. And it notes that death notifications should always be made in person, even if the family doesn't live in the same jurisdiction.

The training—based on best practice standards and the latest research—covers a variety of considerations, including mass casualty events, foreign national victims living in the U.S. and American citizens living abroad, language barriers and other cultural differences, dealing with children and the elderly, the role of victim assistance, the media, and the impact of social media. It features a resource section with web links, a pocket guide for the death notification team to use, and a grief brochure that can be left with the family after the notification. A second video included in the training involves reenactments of proper death notifications.

An assessment tool is also part of the training, and once users receive a passing score, they will be issued a certificate. Questions on the training can be directed to

[deathnotification@leo.gov](mailto:deathnotification@leo.gov).

The FBI's Critical Incident Response Group, Office of Partner Engagement, and Office for Victim Assistance worked together to develop this valuable training with representatives of PSU's Police and Public Safety group and WPSU, the university's public broadcasting entity.

According to Kathryn Turman, head of the FBI's Office for Victim Assistance, there is a nationwide need to provide training for performing proper death notifications so that, echoing Comey sentiments, "victims and their families have the best of us at the worst of times." She added, "We can never underestimate the power of carefully chosen words delivered compassionately."



FBI Director James Comey speaks at the event announcing the new online death notification training, held during National Crime Victims' Rights Week.

# Community Partners Recognized

## 2014 Director's Community Leadership Awards



Left: Recipients of the 2014 Director's Community Leadership Award pose with FBI Director James Comey.

Creating community programs that empower at-risk youth. Providing support for refugees from war-torn countries. Training child protective services personnel, health care workers, and other professionals to provide assistance to victims of human trafficking. Strengthening the academic experience for students in struggling schools.

Today at FBI Headquarters, 57 individuals and organizations from around the nation were recognized by Director James Comey for making extraordinary contributions—like those noted above—to education and to the prevention of crime and violence.

The Bureau has been presenting its Director's Community Leadership Awards (DCLA) for more than two decades to ordinary citizens and organizations striving to build stronger, safer, and more cohesive communities.

Comey said that there are two reasons for presenting these awards every year. First, it's an acknowledgement of the fact that part of the FBI's work of contributing to the protection of communities around the country

is to "build partnerships with other people who are all about the protection of the community." And second, the awards enable the Bureau to hold the recipients up as role models of "what being a citizen really looks like, what being part of a community really looks like."

This year's DCLA honorees, as in past years, were selected by FBI field offices and represent many different sectors—non-profits, business, military, academia, the clergy, behavioral sciences, the media, sports, and civic groups. But while their backgrounds may differ, they all have the same goal: Change their communities for the better and make a positive difference in the lives of other people.

Among those we honor today for their selfless actions:

- A first generation Japanese-American—and Congressional Medal of Honor recipient—who mentors young students at a number of multi-cultural schools in New Mexico and inspires them to be good citizens;
- An anti-violence group in North Carolina that works with a police

department to target violent offenders with focused messages about the impact of violence and offers to help them turn their lives around;

- A marketing professional in Indiana who uses her expertise to help law enforcement solve cold cases, bringing justice for victims and ensuring closure for families;
- A Florida doctor who works to facilitate cooperation and goodwill between the Sikh community and local law enforcement;
- A Kentucky man who works to provide a full range of services to refugee and immigrant families moving into the city to help them successfully integrate into the community;
- An Oklahoma woman who has worked tirelessly on behalf of consumers (particularly seniors) who have been victimized by financial fraudsters; and
- A California organization that offers a variety of prevention and intervention programs to support victims of human trafficking.

Comey noted the diversity of the Director's Community Leadership Awards recipients—the "diversity of good in America," he called it. He added, "I was struck by how many different people from different backgrounds, with different heritages and different traditions, were all doing good but in so many different ways."



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/dcla2014](http://www.fbi.gov/dcla2014).



# Next Generation Crime Stats

UCR's NIBRS Can Offer Fuller Crime Picture



Offense Category	Incidents <sup>1</sup>	Offenses	Victims <sup>2</sup>
<b>Total</b>	<b>4,927,535</b>	<b>5,665,902</b>	<b>5,980,569</b>
<b>Crimes Against Persons</b>			
Assault Offenses	1,120,614	1,289,799	1,289,799
Homicide Offenses	1,032,183	1,193,908	1,193,908
Human Trafficking Offenses	3,562	3,841	3,841
Kidnapping/Abduction Offenses	6	6	6
Sex Offenses, Nonforcible	13,898	15,737	15,737
Sex Offenses, Forcible	65,192	70,144	70,144
Crimes Against Property	5,778	6,163	6,003
<b>Total</b>	<b>3,664,465</b>	<b>3,978,789</b>	<b>2,335,827</b>

"I believe that NIBRS is the pathway to better data—to richer data—that we can all use to have informed conversations about the most important issues we face."

That statement by FBI Director James Comey regarding the FBI Uniform Crime Reporting Program's National Incident-Based Reporting System, or NIBRS, was part of a speech he delivered recently to the National Organization of Black Law Enforcement Executives on the topic of law enforcement and race. To help address the issue more effectively, Comey called for better reporting of incidents where force is used by—as well as against—police. He noted that current demographic data regarding officer-involved shootings is not consistently reported to the FBI's Uniform Crime Reporting (UCR) Program because reporting is voluntary for police departments.

The desire to enhance the quality and quantity of the crime data collected throughout the nation is not new. Back in the 1980s, the Bureau—working directly with our law enforcement partners to help us improve UCR—took advantage of a rapidly changing data processing environment to create a system that would capture more detailed information on individual crime occurrences. All of this additional detail would, collectively, paint a more comprehensive picture of crime on a national level.

***The Bureau is undertaking a number of efforts to educate law enforcement and others on the benefits of NIBRS and to increase participation in the program.***

NIBRS was officially implemented in 1989. While there have been agencies submitting NIBRS data since then—mostly through their state UCR programs—still not enough do so to report on it from a national perspective. Explains Assistant Director Stephen Morris, who heads up our Criminal Justice Information Services (CJIS) Division, "The biggest challenge for any agency, whether you're a local police department or a state program office, is the resources needed to convert systems to NIBRS and the personnel needed to oversee those systems."

The Bureau is undertaking a number of efforts to educate law enforcement and others on the benefits of NIBRS and to increase participation in the program. For example, CJIS is in discussions with its multi-agency Advisory Policy Board about the possible expansion of data to include non-fatal line-of-

## Side by Side UCR Comparison

### *National Incident-Based Reporting vs. Traditional Summary Reporting*

NIBRS	Summary Reporting System
Detailed data collected in 24 categories that include 52 offenses	Aggregate data collected in 10 offense categories
In multi-offense incident, up to 10 crimes are counted	In multi-offense incident, hierarchy rule comes into play—only the most serious crime is counted
Incident-level details captured include the date, time, location and circumstance of the incident as well as characteristics of the victim and offender such as the age, sex, race, and ethnicity	Limited incident-level detail collected for homicides only
Provides a statistical dataset which provides an analysis of the attributes of crime, the correlation of crimes with other demographic factors, and a source of information on a variety of factors affecting crime rates	Does not provide
Detailed data enables agencies to find similarities in crime fighting problems across neighboring jurisdictions which allows them to work together to develop solutions/strategies	Does not enable
Flexible and adaptable to new classifications, modifications, and updates	Cumbersome and inflexible for updates and modifications

duty shootings by law enforcement and about transitioning to a NIBRS-only data collection. We have also partnered with the Department of Justice's Bureau of Justice Statistics on the National Crime Statistics Exchange, or NCS-X, to assist states and agencies interested in submitting their crime data through NIBRS. Said Morris, "You're never going to have 18,000 agencies providing data, but if you have most of the major organizations and they're geographically dispersed, we'll be statistically sound as far a national picture of crime goes."

Unlike UCR's traditional Summary Reporting System (SRS), which is an aggregate monthly tally of crimes in just 10 offense categories, NIBRS captures—in 24 categories—specific details about crimes and criminals, such

as the date, time, location, and circumstance of the incident as well as characteristics of the victim and offender—such as age, race, sex, ethnicity, and any information about their relationship to one another. "NIBRS has the ability to give you the who, what, when, where, and sometimes the why of a crime," added Morris.

Another key difference between the SRS—which has been in operation since the 1930s—and NIBRS is this: Under SRS, during an incident involving multiple offenses, only the most serious crime is reported (i.e., a murder that took place during a robbery would be counted, but the robbery would not). But in NIBRS, both the murder and the robbery would be reported, giving us a more accurate accounting of crime.

When used to its full potential, NIBRS will be able to identify with precision when and where crime takes place, the form it takes, and the characteristics of its victims and perpetrators. Armed with this information, law enforcement agencies can better define the resources they need and apply them where they're needed most. And legislators, municipal planners, academicians, sociologists, advocacy groups, and the public gain access to more extensive crime data as well.

"And at the end of the day," said Morris, "NIBRS will also be able to provide two important elements to law enforcement agencies that have become so important—accountability and transparency."



# Profits Over Safety

## Egg Company's Fraudulent Practices Put Public at Risk

The 81-year-old owner of an Iowa egg production company and his son, a top executive in the business, are going to prison for bribing a federal food inspector and distributing eggs that contained Salmonella bacteria, which caused hundreds of consumers to become sick.

A federal judge in Iowa last month ordered the Quality Egg company to pay a \$6.79 million fine and sentenced company owner Austin “Jack” DeCoster, and his son, Peter DeCoster, who was Quality Egg’s chief operating officer, to serve time in prison.

During the spring and summer of 2010, adulterated eggs produced and distributed by Quality Egg were linked to nearly 2,000 consumer illnesses in a nationwide outbreak of salmonellosis that led to the recall of millions of eggs produced by the defendants.

“This was a classic case of putting profits over public safety,” said Special Agent Grant Permenter, who helped investigate the case from the FBI’s Omaha Division.

Quality Egg pled guilty to bribing an inspector of the U.S. Department of Agriculture (USDA) to release eggs that had been retained for quality issues. The eggs had been “red tagged” for failing to meet minimum USDA quality grade standards. The company also pled guilty to introducing misbranded eggs into interstate commerce with the intent to defraud. From approximately 2006 until 2010, Quality Egg employees affixed labels to egg shipments that indicated false expiration dates with the intent to mislead state regulators and retail egg customers regarding the true age of the eggs.



In the government’s sentencing memorandum prepared for the court, it was noted that Quality Egg personnel had for years disregarded food safety standards and misled customers about the company’s food safety practices.

*“It seems obvious that company profits outweighed other concerns.”*

“As with a lot of fraud cases,” Permenter said, “Quality Egg’s crimes were committed over and over for years, and, eventually, these illegal practices caught up with them.” But this case was not just about deception, he said. “People got sick. There was a serious public safety issue here. Quality Egg’s business practices put the public at risk—at times, substantial risk.”

Permenter explained that the FBI assisted in the investigation led by the USDA’s Office of Inspector General and the Food and Drug Administration’s Office of Criminal Investigations. He added

that the USDA inspector who received bribes from Quality Egg was in ill health and died before he could be charged. “The inspector was a federal employee. Had he lived,” Permenter said, “he would have been charged and, in all likelihood, would have gone to jail as well.”

In June 2014, Quality Egg and Jack and Peter DeCoster pled guilty to bribery and other charges related to adulterated egg distribution.

In the end, Permenter said, “it seems obvious that company profits outweighed other concerns.” By being able to circumvent the inspection process through bribes and not having to remove the tainted eggs from its inventory, the company saved a significant amount of money. “When you start bending your ethical and moral fibers because there are dollar signs in front of you,” he said, “a lot of bad things are likely to happen.”

# Alabama Jeweler Sentenced in Federal Court

## Caught Pawning His Own ‘Stolen’ Diamonds



Clockwise, from top left: Sapphire and diamond necklace with a 27-carat ceylon blue sapphire worth \$91,000; pair of 2.5 carat platinum Asscher-cut diamond stud earrings and yellow gold jackets worth \$75,000; platinum 2.39 carat solitaire diamond ring worth \$36,500; loose 1.11 carat oval “blue diamond” worth \$620,000.

A warning to criminals: No matter how long it takes or how careful you are, law enforcement will eventually come knocking.

Back in December 2004, local police responded to a report of an armed robbery at a jewelry store in Mountain Brook Village, Alabama. The account from the store’s owner—Joseph Harold Gandy—was a frightening one: Two men had entered just before closing time, first asking to look at an expensive watch but then pulling out guns and threatening the owner and his employee. They tied up the employee, forced Gandy to empty the contents of the display cases into a bag, and then tied up the owner and fled the store with the stolen merchandise.

After a months-long investigation, the Mountain Brook Village Police Department began to think that the robbery may have been an inside job. Even though the store was located on a very busy street, there were no other witnesses to the crime. The robbers had conveniently taken the store’s security camera. Not long before the robbery, the owner had increased his insurance coverage. And most of the stolen jewelry items had recently been added to the store’s inventory, on consignment from jewelers in New

York and elsewhere for a “loose diamond sale” just before the holidays.

The total value of the merchandise supposedly stolen—reported by Gandy to his insurance company—was \$2.8 million. The insurance company paid out \$2.6 million, the policy’s limit.

Investigators from the Mountain Brook Village Police Department took their suspicions to the Birmingham FBI Office and asked for assistance. But over time, investigative efforts weren’t able to uncover any hard evidence of what local police suspected. That is, until 2013, when we received a tip that Gandy had begun pawning some of the diamonds he had reported stolen nine years earlier.

His first attempt, in July 2013, was unsuccessful. Gandy had asked a friend to take a one-and-a-half carat diamond to another jewelry store to pawn it. The very conscientious jeweler at that store asked for documentation and began looking at the stone a little too closely. Gandy had concerns that the diamond might bear a unique laser inscription (certain numbers, letters, logos, etc.) that would enable the jeweler to trace its origins—so the transaction was not completed. Going forward, Gandy made sure that he first examined

the diamonds he was trying to pawn under a microscope and selected ones without inscriptions.

Between August and November 2013, Gandy’s friend pawned two more large diamonds: a 3.45-carat one and a 2.16-carat one. Both stones were on the stolen inventory list Gandy had sent to his insurance company in 2004.

By November 2013, law enforcement had what it needed to go after Gandy. Armed with a search warrant, the FBI and the Vestavia Hills Police Department went to his Vestavia Hills home and recovered some of the jewelry he had previously reported stolen. As a bonus, we also found a cache of 99 weapons in the home—Gandy, convicted on a federal mail fraud charge years earlier, was prohibited from possessing firearms.

Last month, as part of a plea agreement, Gandy was sentenced to a federal prison term on charges of money laundering related to the pawning of or property worth more than \$10,000 that he had obtained through a criminal act. That criminal act? Wire fraud, which he committed nine years earlier when he submitted his phony insurance claim. He was also charged with the firearms violation.

We were never able to determine why Gandy waited so long to pawn the jewelry he had bogusly reported as stolen, but we do know that he told an acquaintance he wanted to open an additional jewelry store. However, thanks to the cooperative efforts of all the agencies involved, and the assistance of the U.S. Secret Service, we were able to uncover and hold Gandy accountable for his illegal and dishonest actions.



# Financial Fraud

## Oklahoma Pastor Embezzled Nearly \$1 Million from Community Center

The long-time pastor of the Greater Cornerstone Baptist Church in Tulsa, Oklahoma was recently sentenced to 37 months in prison for embezzling close to \$1 million from a community center he helped establish to aid the church's struggling neighborhood.

Willard Leonard Jones essentially had an "open checkbook" for the church and community center accounts, said Special Agent Kevin Legleiter, who investigated the case with Forensic Accountant Janetta Maxwell from the FBI's Oklahoma City Division. The two have partnered on financial fraud investigations for 20 years, and after following the paper trail in this case, there was no doubt of the reverend's criminal activity.

"People trusted him and assumed he was doing the right thing," Legleiter said. Instead, Jones used approximately \$933,000 of community center money for his personal benefit—to pay his mortgage, buy luxury items like a Rolex watch, and to live a lavish lifestyle that included gambling and expensive hotel accommodations.

In 2004, Jones had the idea to build a community center not far from his church in a disadvantaged West Tulsa neighborhood called South Haven. The center would bring health care, a food and clothing bank, and other resources to the community. As the executive director of the Greater Cornerstone Community Development Project, Jones solicited donations from foundations, corporations, churches, and individuals—and raised about \$7 million.

"It was his vision," Maxwell said. "He started the project and raised funds for it." But as the money came in, Jones began transferring



The Cornerstone Community Center in Tulsa, Oklahoma sits largely empty due to the embezzlement of nearly \$1 million in funds meant for the project by the pastor who helped establish it.

funds from community center bank accounts to church bank accounts—and then transferred funds into his personal accounts.

After the center was completed in 2012, Jones went to the board of directors and said he needed more money. Surprised by the lack of funds, the board sought an audit and learned about center funds being transferred into church accounts. Jones said he did that to get a tax exempt status for some of the contractors. When the board asked to audit the church accounts, Jones refused, and the board filed a police report.

The FBI was asked to assist in the investigation. Legleiter and Maxwell began a painstaking look at the financial transactions involved over a six-year period. In one account alone, Maxwell said, there were 10,000 entries that needed to be analyzed.

In 2013, Jones was charged federally with three counts of wire fraud and one count of filing a false tax return. Federal charges were brought because in the process of

transferring funds from the center to the church and then to his own accounts, the funds were routed electronically through another state.

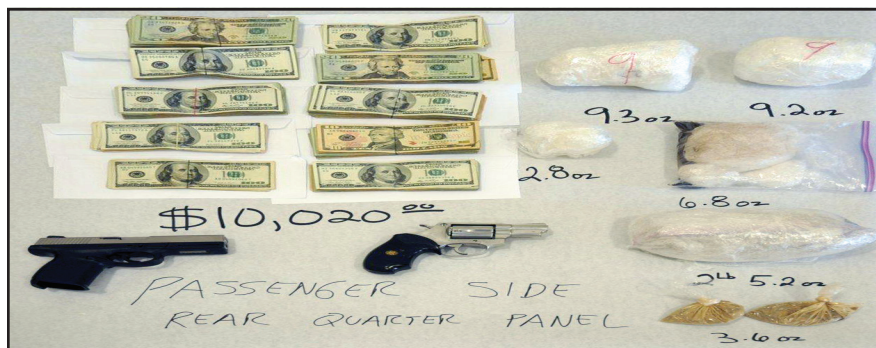
"When there is an interstate wire transfer that involves fraud," Legleiter explained, "the FBI has jurisdiction over that. We also partnered with the IRS because if, in fact, Jones received money that he didn't claim on his taxes, that would be a tax violation."

Ultimately, Jones admitted that from 2007 to 2013, he misappropriated the funds and also failed to report nearly \$400,000 to the IRS. He was sentenced to prison in January.

Legleiter and Maxwell said a lack of internal controls on the part of the church and the community center enabled the embezzlement to go on for so long. Today, the community center—a beautiful facility that sits in the shadow of the Greater Cornerstone Baptist Church—is largely empty because there are no funds to operate it.

# Leader of Violent California Gang Sentenced

## Operations Financed Through Drug and Firearms Trafficking



Left: The cash, weapons, and drugs seized from a hidden compartment in the so-called “trap car” used by California drug trafficker and gang leader Luis Manuel Tapia.

Luis Manuel Tapia was a high-powered leader of one of Ventura County’s largest and deadliest gangs—the Colonia Chiques. He was often heard encouraging younger gang members to assault rival gang members, kill suspected informants, enhance the gang’s drug and weapons trafficking operations, and maintain territorial dominance by any means possible.

But after an extensive investigation by the Ventura County Violent Crimes Task Force—made up of FBI agents and officers from the Oxnard and Ventura Police Departments—Tapia, 39, was convicted by a federal grand jury in Los Angeles and sentenced last month to six life terms without parole plus an additional 55-year consecutive term. Four other key Colonia Chiques members and associates who were charged with Tapia previously pled guilty. (A fifth person charged is a fugitive believed to be in Mexico.)

The Colonia Chiques became the focus of the Ventura County Violent Crimes Task Force because of the vast number of violent crimes committed by its members and because of the group’s alignment with the extremely violent Mexican Mafia, a powerful gang within the California prison system. In return for helping the Mexican Mafia carry out its illegal activities (involving drugs, weapons, etc.)

inside and outside prison walls, Hispanic gangs like the Colonia Chiques who align themselves with the Mexican Mafia get a cut of the group’s illegal profits and are promised protection when their members find themselves behind bars. Tapia’s relationship with the Mexican Mafia helped him import high-quality, often deadly drugs from Mexico.

In Ventura County and surrounding areas, Colonia Chiques members were involved in a wide variety of violent and serious crimes—murders, attempted murders, drive-by shootings, assaults with deadly weapons, drug trafficking, firearms trafficking, robberies, burglaries, and car thefts. The level of violence they perpetrated made the public fearful to report crimes committed by the gang, testify against Colonia Chiques members, and visit areas of town frequented by gang members.

At the center of it all was Tapia, leading, directing, and managing his criminal enterprise and his crew. Tapia, in an acknowledgement of his lynchpin role, was once overheard boasting, “I know how it feels to be a CEO.” But by combining the efforts and the expertise of the Bureau, our partners on the task force, and federal prosecutors, we were able to knock Tapia out of his perch and do serious harm to his organization.

The jury at Tapia’s trial heard a lot about the activities of the Colonia Chiques—much of it from Tapia himself in the form of audio and video recordings captured by law enforcement. For instance:

- “I killed a lot of people [with my heroin], it was so strong...it was good advertisement.”
- “Whatever you need...I’m like the black market.”
- “I got good access to a lot of [illegal product]...as long as you know who you’re messing with.”

Confidential informants provided us with a wealth of critical information on Tapia. We also used undercover scenarios against him and his group—one in particular where an FBI agent posed as a senior member of the Italian Mafia and negotiated to have Tapia supply the Las Vegas syndicate of the Mob with a monthly supply of methamphetamine.

By the end of the trial, members of the jury were convinced enough to convict him on all 26 charges.

The prosecutions of Tapia and his associates are part of a larger joint effort by law enforcement to target the Colonia Chiques and other Ventura County street gangs affiliated with the Mexican Mafia. In 2011, a total of 11 gang defendants were convicted in federal court and received sentences of up to 25 years each. And in November 2013, 17 more gang members were charged with drug distribution.

As a result of these actions, the streets of Ventura County are a little safer these days.



# Help Us Find Them

## National Missing Children's Day 2015

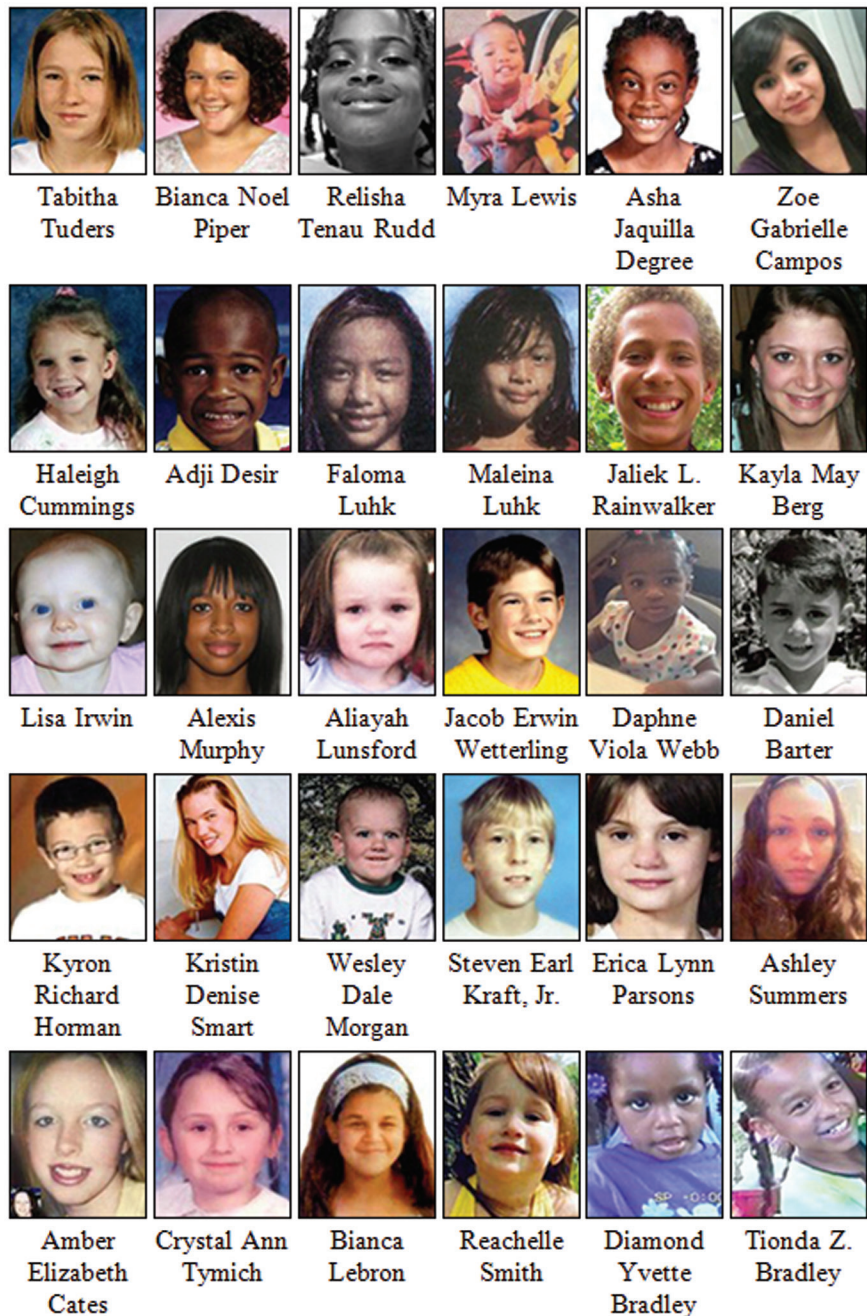
On May 25, 1979, 6-year-old Etan Patz disappeared while walking to his school bus stop in New York. Four years later, to honor Etan's memory and the memories of other missing children, President Ronald Reagan proclaimed May 25—the anniversary of Etan's disappearance—as National Missing Children's Day.

Tragically, however, children continue to disappear, and as we approach National Missing Children's Day 2015, the FBI would like to ask the public for its continued help in locating any of the young victims pictured above from our Kidnapping and Missing Persons webpage.

According to Director James Comey, "The FBI remains vigilant in its efforts to eradicate predators from our communities and to keep our children safe." In addition to working with our law enforcement partners to publicize the names and faces of missing children, the Bureau undertakes a variety of efforts to help rescue the most vulnerable of victims. For example:

- Rapid response teams are stationed across the country to quickly respond to child abductions.
- Our investigators can offer a full array of resources such as DNA analysis, trace evidence, impression evidence, and digital forensics tools.
- Through improved communication, we can quickly share information with law enforcement partners around the world.

As for Etan Patz—the little boy whose name and face have become synonymous with this issue—he has never been found.



But as a result of law enforcement efforts and the public's assistance, other youngsters have been safely recovered and returned to their families, or at the very least, their families have been given some degree of closure.

And we will continue to look for these children—seeking justice for them and for their families—no matter how long it takes. Despite the fact that the court proceedings

of a suspect believed responsible for Etan Patz's disappearance nearly 36 years ago ended in a mistrial earlier this month, prosecutors have announced they will retry the case.

*Note: The children pictured here may have been located since the above information was posted on our website. Please check [www.fbi.gov/wanted](http://www.fbi.gov/wanted) for up-to-date information.*



# International Soccer Officials Indicted

*'Deep-Rooted' Corruption, Racketeering Alleged*



FBI Director James Comey joins other federal officials, including Attorney General Loretta Lynch (left) at a press conference in New York regarding the indictments of nine FIFA officials and five corporate executives on corruption and racketeering charges.

The U.S. government this morning unsealed indictments in a New York federal court against high-ranking officials and corporate executives affiliated with FIFA, the governing body of international soccer, for their roles in a decades-long scheme to corrupt the sport through bribes, kickbacks, and other criminal activity aimed at controlling lucrative marketing rights to international tournaments such as the World Cup.

Nine FIFA officials—including two current vice presidents—along with five corporate executives were charged with racketeering, wire fraud, and money laundering, among other offenses.

“The indictment alleges corruption that is rampant, systemic, and deep-rooted both abroad and here in the United States,” said Attorney General Loretta E. Lynch. “It spans at least two generations of soccer officials who, as alleged, have abused their positions of trust.”

Related guilty pleas of an additional four individuals and two corporate defendants were unsealed today as well. The investigation, which is ongoing, has also snared U.S. sports marketing executives. In all,

it is alleged that more than \$150 million in bribes and kickbacks were paid or agreed to be paid to obtain media and marketing rights to international soccer tournaments.

“The defendants fostered a culture of corruption and greed that created an uneven playing field for the biggest sport in the world,” noted FBI Director James B. Comey. “Undisclosed and illegal payments, kickbacks, and bribes became a way of doing business at FIFA,” he said.

FIFA—the Fédération Internationale de Football Association—is the organization responsible for the regulation and promotion of soccer worldwide. It also oversees officials of other soccer governing bodies that operate under the FIFA umbrella.

*“...Illegal payments, kickbacks, and bribes became a way of doing business at FIFA.”*

The organization is composed of 209 member associations, including six continental confederations that assist it in governing soccer in different regions of the world. The U.S. Soccer Federation is one of 41 member associations of the confederation known as CONCACAF, which has been headquartered in the U.S. throughout the period charged in the indictment.

A key way FIFA makes money is by selling media and marketing rights associated with flagship tournaments such as the World Cup. Rights are typically sold through multi-year contracts. Sports marketing companies, in turn, sell the rights downstream to TV and radio broadcast networks,

major corporate sponsors, and other sub-licensees who want to broadcast the matches or promote their brands. According to FIFA, 70 percent of its \$5.7 billion in total revenues between 2011 and 2014 was attributable to the sale of TV and marketing rights to the 2014 World Cup.

The indictment alleges that between 1991 and present, the defendants and their co-conspirators corrupted the enterprise by engaging in various criminal activities. Two generations of soccer officials abused their positions of trust for personal gain, frequently through alliances with sports marketing executives who shut out competitors and kept highly lucrative contracts for themselves through the systematic payment of bribes and kickbacks.

The investigation was carried out by the FBI's New York Field Office—specifically the Eurasian Joint Organized Crime Squad—in partnership with the Internal Revenue Service's Criminal Investigation Division and a variety of international partners.

The wide-ranging corruption at FIFA, said Lynch, “has profoundly harmed a multitude of victims, from the youth leagues and developing countries that should benefit from the revenue generated by the commercial rights these organizations hold, to the fans at home and throughout the world whose support for the game makes those rights valuable. Today's action,” she added, “makes clear that this Department of Justice intends to end any such corrupt practices, to root out misconduct, and to bring wrongdoers to justice. We look forward to continuing to work with other countries in this effort.”



# Taken for a Ride

## Travel Agent Scammed Marching Bands Out of Trips

The trip to Hawaii for 270 high school band members and their chaperones was supposed to be the crescendo of months of performances, fundraisers, and saving to book the arrangements. But the music stopped when the band's travel agent admitted he'd duped them to the tune of more than \$272,000.

In August 2011, a high school band in Arkansas contracted with Utah-based travel agent Calliope R. Saaga to arrange the once-in-a-lifetime trip. The school wired the funds in multiple installments, but rather than booking the band's Hawaii excursion, Saaga spent the money himself—on his own trips to Disneyland, Samoa, and Las Vegas—all the while offering assurances the band's trip was on schedule. It wasn't until Saaga stopped answering calls after the last payment in February 2012 that school officials got suspicious. Soon after, just months before their scheduled departure, Saaga admitted he'd lost all their money.

"I made some terrible decisions with the money," Saaga said in a 2012 e-mail to the band's assistant director, who had booked two trips previously with Saaga so was shocked by the turn of events.

"They thought they had someone they could trust," said Special Agent Tim Akins of the FBI's Little Rock Division, which opened a wire fraud case against Saaga. "Now all of a sudden they don't have money to go anymore."

It got worse. During Akins' investigation, he learned that the FBI's Kansas City Division had opened its own case on Saaga after a Missouri high school said the travel agent had bilked its band boosters out of more than \$360,000



for a Hawaii trip. The Bureau's Springfield (Missouri) Division was also looking into Saaga. Then emerged still another scheme by Saaga to cheat an Arkansas school district. Forensic accounting in the Kansas City case showed Saaga spent at least 47 days gambling in Las Vegas when he should have been booking the schools' outings.

"Saaga is a thief who stole from hard-working citizens and their children," said FBI Little Rock Special Agent in Charge David T. Resch.

During the course of the investigation, Saaga fled to Samoa, where he is from. In his e-mail admission to the band director, he said he was trying to sell his assets there to repay the group. "It will be a slow process so I beg of your patience," he wrote.

Parents who had been duped hoped Saaga would face justice and expressed frustration on social media. In a May 2012 message on a Samoa news outlet's Facebook page, the mother of a band member said families had worked hard to fund their summer trip. "Some of the kids took on part time jobs to pay for this trip," the mother said,

"others even borrowed money from the bank."

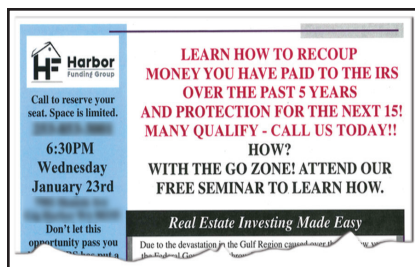
Saaga ultimately returned to the U.S. to face multiple wire fraud and money laundering charges for schemes that resulted in more than \$700,000 in losses. He was indicted in May 2014. Among his scams:

- Stealing \$360,000 from Willard High School Band Boosters (Springfield, Missouri), forcing the cancellation of a trip to Hawaii for more than 300 students and chaperones.
- Stealing \$272,500 from Southside High School (Fort Smith, Arkansas), forcing the cancellation of a Hawaii trip for 270 marching bands students and their families.
- Stealing \$149,000 from a school district in West Memphis, Arkansas.

Saaga was sentenced March 12 to five years in federal prison in the Willard High school case. On March 31, he was sentenced to 63 months for swindling Southside High School's band. The sentences are to run concurrently. He was also ordered to pay \$780,000 in restitution.

# Financial Fraud

## Lengthy Prison Term for Advance Fee Fraudster



Like many successful con men, William C. Lange made people believe that he really cared about them—even as he looked them in the eye and took their money.

The 67-year-old Washington state businessman was sentenced in March to 22 years in federal prison for swindling more than 300 investors in the U.S. and overseas out of \$10 million. He had befriended some of his victims at Rotary Club functions. Many thought they would be getting loans to rebuild after the devastation of Hurricane Katrina in 2005.

“Unfortunately, this type of white-collar crime is all too common,” said Special Agent Ben Williamson, who investigated the case with Special Agent Mike Brown from the FBI’s Seattle Field Office. “Some investors lost their life savings.”

Lange and his co-conspirators, including his son, operated two companies that were “based entirely on lies,” Brown said. Lange founded the Harbor Funding Group, Inc. (HFGI) in 2006, and not long after began to target real estate developers and their clients seeking to rebuild after Hurricane Katrina. The pitch was that HFGI had access to lenders and millions of dollars in funds to finance real estate projects. To get that money, however, HFGI required investors to place 10 percent of the loan amount in an escrow account.

**Left: William Lange’s Harbor Funding Group, Inc. placed ads such as this to target real estate developers and their clients seeking to rebuild after Hurricane Katrina. Instead of financing their projects, however, Lange swindled hundreds of people out of millions of dollars.**

In reality, HFGI had neither lenders nor funds. And as soon as the money was placed in escrow, Lange took it to finance his own lavish lifestyle.

That advance fee scheme netted more than \$9 million, which Lange spent on salaries, fishing and hunting trips, landscaping for his new house, Harley-Davidson motorcycles, and other business ventures. After the money was gone, Lange set up another sham business—Black Sand Mine, Inc. (BSMI)—with the supposed intention of mining gold and other precious metals on an Alaskan island.

Beginning in 2009, Lange convinced investors—through lies and misrepresentations—to purchase BSMI stock. Almost \$1 million was collected, but instead of using it to mine for gold, the money was spent on salaries and other personal expenses for Lange and his crew.

The FBI began to receive complaints about Lange’s business dealings, and in 2009 partnered with the U.S. Postal Inspection Service, which had also begun looking into his activities. During the investigation, countless financial documents were reviewed, victims were interviewed, and cooperating witnesses were engaged to help unravel the frauds. Lange was arrested in 2011.

In September 2014, Lange pled guilty to conspiracy to commit wire and securities fraud and admitted his leadership role in both the

advance fee fraud and the gold mine investment schemes. Other co-conspirators have already been convicted or pled guilty in related cases, Williamson said, “but clearly Lange was the mastermind behind these crimes.”

Both Williamson and Brown are pleased that Lange received a lengthy jail term, but they also remember the hundreds of victims in the case.

One individual who lost nearly \$100,000 in the HFGI scheme wrote in a victim impact statement for the court, “Our life savings have gone—we have nothing. Life financially has been horrific for us.” Another HFGI victim wrote, “We live in England, and this property investment opportunity was widely publicized here as a way to make a positive contribution to rebuilding the Katrina affected area as well as making a financial return.”

“We are glad that Lange is off the streets,” Brown said, “and unable to victimize anyone else.”

### How to Avoid Becoming a Victim

FBI agents who specialize in financial fraud stress that investors need to exercise common sense before giving someone their money. “There are no quick ways to get rich,” said Special Agent Ben Williamson. “If an investment opportunity seems too good to be true, it probably is.”

Before investing your money, it’s always a good idea to:

- Do your research. Who are you dealing with? Check for complaints with the Better Business Bureau and elsewhere online.
- Talk to as many people as you can about the investment. Get second opinions.
- Don’t rush into any decisions.
- If you are engaging in risky investments, be willing to lose what you put in.



# Serial Armed Robber Gets Substantial Prison Term

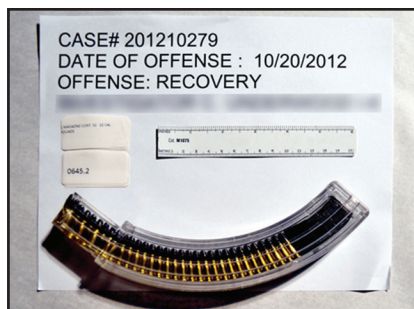
## Joint Law Enforcement Effort Pays Off

It was a highly effective combination of local and federal resources. A 38-year-old man was identified by local police as the suspect in a series of frightening armed robberies of businesses in the Birmingham, Alabama area, one of which ended with a customer getting shot. Local authorities contacted the FBI's Birmingham Field Office with a request for assistance—they wanted to see if their suspect could be charged under the federal Hobbs Act, taking advantage of its harsher penalties.

The multi-agency investigation that followed led to this particular suspect—Jamey Lee Matthews—pleading guilty to four counts of robbery under the Hobbs Act. And just last month, he received a 25-year federal prison term. The judge also ordered him to pay \$208,000 in restitution to the man he shot and to the stores he robbed.

The series of robberies Matthews was charged with took place during October 2012, and among the businesses he robbed were a convenience store, a dollar store, a supermarket, a pharmacy, and a gas station. His first job was the convenience store, which he entered just after 4 a.m. on October 11, 2012, with a shotgun. He threatened the female clerk, who complied with his order to open the register. Subsequent robberies were similar—he would enter the store with a firearm, often wore a Halloween mask, threatened employees and customers, and demanded money.

At the pharmacy he robbed, he varied his routine—rather than demanding money, he demanded prescription medication and ended up with more than 3,000 pills containing controlled substances.



But things took a potentially deadly turn the night of October 19, 2012, when Matthews entered a gas station with the intent to rob it. After brandishing a gun and threatening violence, employees gave him the money and he left. Several employees and a customer chased him, though, and Matthews fired at them, hitting the customer five times and severely wounding him.

The story took another turn the next morning, when a seriously injured man was found beneath a remote bluff outside of Birmingham and taken to a hospital. Local law enforcement responding to the scene found a pickup truck a short distance away with various firearms leaning up against the vehicle and others on the ground nearby, as well as evidence inside the truck seemingly tied to the series of Birmingham robberies. The truck was registered to a Birmingham woman who was the mother of the man found under the bluff. That man was Jamey Lee Matthews, and police soon honed in on Matthews as their suspect.

The federal investigation was led by the FBI and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), ably assisted by the Birmingham Police Department, the Blount County Sheriff's Office, and our partners on the Northern Alabama Safe Streets Task Force, the Jefferson County Sheriff's Office.

**Left: Shown is a clear ammunition magazine for one of the firearms seized from Birmingham armed robber Jamey Lee Matthews. The unique attributes of some of the weapons Matthews used during the robberies—like a clear magazine—helped eyewitnesses to better identify them.**

According to the FBI Birmingham case agent, the investigation had complicating factors: the necessity of meeting the Hobbs Act threshold, the shooting during the gas station robbery, the pharmacy theft (also a federal offense), etc.

But working in investigators' favor was the fact that Matthews wore memorable Halloween masks during most of the robberies—including one of a devil—and that the firearms he used stood out—one gun had a clear ammunition magazine, some had different colored tape, another was a silver sawed-off rifle, and another was an Uzi-style weapon. The distinguishing masks and firearms made it easier for eyewitnesses to describe what they had seen, and their accounts were often supported by store surveillance video.

And among the items seized from the pickup truck and from Matthews' mother's house were some of those firearms and masks matching eyewitness descriptions, clothing similar to what the robber had worn, a customer's check written out to the victim gas station, and prescription bottles from the victim pharmacy.

In the face of such overwhelming evidence, Matthews agreed to plead guilty. And a joint law enforcement endeavor resulted in getting another dangerous criminal off the streets for a very long time.

# The Case of the Corrupt Coin Dealer

Fraudster Targeted Elderly Victims



Financial fraud comes in all shapes and sizes. And while corporate criminals, inside traders, and Ponzi schemers often cause their victims to lose millions of dollars, the case of the crooked coin dealer from New York illustrates that even relatively small-time fraudsters must answer for their crimes.

Chrysanthos Nicholas, a 55-year-old rare coin and precious metals dealer, will be spending the next 27 months in federal prison for stealing more than \$260,000 from some of his elderly customers.

Nicholas had been a coin dealer for a number of years and had developed relationships with collectors around the country. He persuaded three elderly clients—all well into their 80s—to send him coins with the promise that he would value them, hold them, and sell them for the clients on their request.

“Such arrangements are not uncommon in the coin collector world,” said Special Agent Shane Ball, who investigated the case from the FBI’s Minneapolis Division. But after the dealer had received coin collections from

the men, “he promptly stopped returning their calls,” Ball said. “He completely dropped off the radar.”

In one case, according to court documents, Nicholas entered into a contract with a client in rural Minnesota to evaluate, store and sell the client’s coins. In 2010, at Nicholas’ direction, the client mailed his coins—valued at more than \$130,000—to Nicholas in Southold, New York.

Later, after Nicholas stopped answering or returning the client’s calls, the victim went to his local sheriff’s office and made a complaint. Because the coin dealer lived outside of Minnesota, the sheriff’s deputy called the FBI for assistance. Ball, a 20-year veteran of the Bureau, explained that agents regularly offer assistance to local law enforcement in these types of matters that cross state lines.

Ball, in turn, requested assistance from the FBI’s New York Field Office, and Special Agent Zacharia Baldwin was dispatched to interview Nicholas.

“My belief is that Nicholas picked these particular victims because

they were elderly and he thought he could get away with it,” Ball said. For their part, the victims had all done business with Nicholas in the past with no problems. “They had every reason to suspect that this was another business deal that would go well,” Ball added. “But Nicholas used the trust he had built up over the years to steal from them.”

Meanwhile, Nicholas sold the coins and used the money for his personal benefit. When he was charged with mail fraud in July 2014, nothing remained of his victims’ collections. At his sentencing last month, a federal judge ordered Nicholas to pay nearly \$250,000 in restitution to his victims after he completes his jail term.

Although the money Nicholas stole from his clients is small compared to some financial frauds, Ball is quick to point out that it represented a great deal to the victims—it was one man’s life savings. “Our goal is always to seek justice for victims,” he said, “whether they are corporate shareholders or individuals from small-town America.”



# FBI Safe Online Surfing Internet Challenge

## Cyber Safety for Young Americans

In April, the Pew Research Center published a study saying that 92 percent of teens report going online daily—including 24 percent who say they go online “almost constantly.” According to the study, nearly three-fourths of teens have or use a smartphone.

Considering the many dangers that lurk on the Internet—from child predators to cyber bullies, from malicious software to a multitude of scams—it’s imperative that our young people learn the ins and outs of online safety from an early age.



The FBI-SOS website features grade-specific islands with age appropriate games, videos, and other interactive materials in various portals.

That is precisely why the Bureau launched the FBI Safe Online Surfing (SOS) Internet Challenge in October 2012 with a dedicated new website. FBI-SOS is a free, fun, and informative program that promotes cyber citizenship by educating students in third to eighth grades on the essentials of online security. For teachers, the site provides a ready-made curriculum that meets state and federal Internet safety mandates, complete with online testing and a national competition to encourage learning and participation. A secure online system enables teachers to register their schools, manage their classes, automatically grade their students’ exams, and request the test scores.

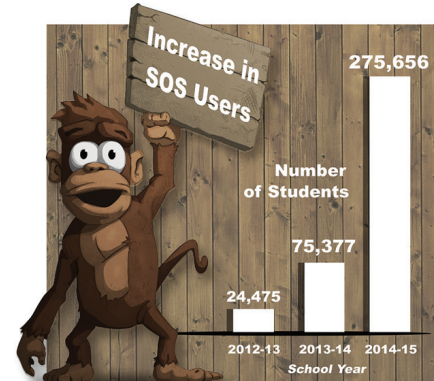
FBI-SOS just finished its third school year, with record results. A total of 275,656 students completed the exams—more than triple the previous year. The competition included 5,053 schools in 49 states, D.C., Puerto Rico, and the Northern Mariana Islands.

“We couldn’t be more pleased with how teachers and students are responding to the program and how participation is growing in such leaps and bounds,” said Scott McMillion of the FBI Criminal Investigative Division’s Violent Crimes Against Children Section, which runs the program in concert with our Office of Public Affairs and field offices nationwide. “FBI-SOS is helping to turn our nation’s young people into a more cyber savvy generation and to protect them from online crime now and in the future.”

*“We couldn’t be more pleased with how teachers and students are responding to the program and how participation is growing in such leaps and bounds.”*

The FBI-SOS website features six islands—one for each grade level—with age appropriate games, videos, and other interactive materials in various portals. The site covers such topics as cell phone safety, the protection of personal information, password strength, instant messaging, social networking, and online gaming safety. The videos include real-life stories of kids who have faced cyber bullies and online predators.

After navigating through the appropriate island, students take



The popularity of our SOS online cyber program has grown over the past several school years. The number of students who have completed the training went from 24,475 in 2012-2013, to 75,377 in 2013-2014, to 275,656 in 2014-2015. That’s a grand total of 375,508 students.

a timed quiz. The test scores for each school are aggregated by the FBI and appear on a national leaderboard on the website each month from September through May. Schools compete in one of three categories, determined by the number of students participating: Starfish (5-50 participants); Stingray (51-100); and Shark (100+). The top-scoring school in each category at the end of the month receives a national FBI-SOS award. When possible, the winning schools are visited by representatives of their local FBI field office.

Anyone—young or old, in the U.S. or worldwide—can complete the activities on the FBI-SOS website. The testing and competition, however, are only open to students in grades 3-8 at public, private, or home schools in the U.S. or its territories.

We’d like to congratulate the 26 schools that won the competition this past year and thank the many teachers and students who participated. We hope you will join us again in September.

# Ten Sentenced in Hate Crime Case

## Murdered Man Among Multiple Victims

In Jackson, Mississippi, in the early morning hours of June 26, 2011, a 47-year-old African-American man—James Craig Anderson—was severely beaten and then intentionally run over with a pickup truck in an unprovoked attack by a group of white teenagers from nearby suburbs. Some of the teens yelled racial epithets during this horrific incident, a random act of hate crime violence that resulted in Anderson's death.

The FBI's Jackson Field Office opened an investigation, and it wasn't long before we were able to piece together a conspiracy among at least 10 individuals who—on a half-dozen or so different occasions—made and carried out plans to target, harass, and hurt African-Americans in Jackson, specifically those they believed were homeless or under the influence of alcohol because they thought that such individuals would be less likely to report the assault.

All 10 were eventually charged with federal hate crimes. And all 10 have pled guilty and were sentenced to federal prison terms ranging from four years to 50 years. The 50-year term went to Deryl Paul Dedmon, the pickup truck driver who ran over Anderson. Dedmon was also charged in state court with murder and received two life sentences.

These hate crime incidents, which began in the spring of 2011 and occurred while the subjects were driving through Jackson—often after an evening of partying—culminated in the June 2011 death of Anderson, an auto plant worker.

Several of the subjects saw Anderson alone in the parking lot of a Jackson hotel. They stopped

their vehicle and—after using cell phones to contact several other subjects who were nearby in another vehicle—got out of the car to distract their victim until their co-conspirators arrived. Once the second vehicle arrived, one individual struck Anderson in the face, knocking him to the ground. A second individual straddled the victim and struck him repeatedly in the face and head with a closed fist. Leaving Anderson lying there, they got back into their vehicles and, urged on by two of the female subjects and yelling a racial epithet, Dedmon ran over the victim on his way out of the parking lot.

Among the other hate crime incidents the subjects were charged with:

- Chasing down and physically assaulting an African-American man walking near a golf course by punching and kicking the victim in the body, head, and face until he begged for his life.
- After locating an African-American man in an empty strip mall parking lot, quickly accelerating their vehicle in an attempt to hit him (fortunately, the man was able to jump out of the way in time).
- Hurling glass beer bottles at targeted victims, in one instance actually knocking a man down with the force.
- Using a sling shot to launch metal ball bearings at various individuals, including a teenage boy riding a bicycle.

After Anderson's death, FBI personnel from the Jackson Field Office formed an investigative team with prosecutors from the U.S. Attorney's Office for the Southern District of Mississippi, the Department of Justice's Civil



The pickup truck that was used to run over and kill James Craig Anderson. The driver of the truck was sentenced to 50 years in federal prison.

Rights Division, and a Special Assistant U.S. Attorney appointed from the Hinds County District Attorney's Office. The extensive investigation involved hundreds of interviews, the execution of search warrants, search and evidence collection by the FBI Evidence Response team, video forensic analysis by the FBI Laboratory, cell phone examinations by the FBI Computer Analysis Response Team, and analysis of telephone records.

Tragically, one of our law enforcement partners in this investigation—Jackson Police Department Detective Eric Smith—was shot and killed by a murder suspect in an unrelated April 2013 incident. Detective Smith was able to uncover a great deal of information in this case in a very short period of time, and his work formed a solid basis for the start of the federal investigation.

Hate crimes have a devastating impact on communities, which is why the FBI remains committed to working with our state and local partners—with the help of the public—to bring to justice those who perpetrate them.



# Health Care Fraud Takedown

## 243 Arrested, Charged with \$712 Million in False Medicare Billings

More than 240 individuals—including doctors, nurses, and other licensed professionals—were arrested this week for their alleged participation in Medicare fraud schemes involving approximately \$712 million in false billings.

The arrests, which began Tuesday, were part of a coordinated operation in 17 cities by Medicare Fraud Strike Force teams, which include personnel from the FBI, the Department of Health and Human Services (HHS), the Department of Justice (DOJ), and local law enforcement. The Strike Force's mission is to combat health care fraud, waste, and abuse.

At a press conference today at DOJ Headquarters in Washington, D.C., officials said the arrests constituted the largest-ever health care fraud takedown in terms of both loss amount and arrests.

"These are extraordinary figures," said Attorney General Loretta Lynch. "They billed for equipment that wasn't provided, for care that wasn't needed, and for services that weren't rendered."

The charges are based on a variety of alleged fraud schemes involving medical treatments and services. According to court documents, the schemes included submitting claims to Medicare for treatments that were medically unnecessary and often not provided. In many of the cases, Medicare beneficiaries and other co-conspirators were allegedly paid cash kickbacks for supplying beneficiary information so providers could submit fraudulent bills to Medicare. Forty-four of the defendants were charged in schemes related to Medicare Part D, the prescription drug benefit program, which is the fastest growing component of Medicare

and a growing target for criminals.

"There is a lot of money there, so there are a lot of criminals," said FBI Director James B. Comey. He described how investigations leveraged technology to collect and analyze data, and rapid response teams to surge where the data showed the schemes were operating. "In these cases, we followed the money and found criminals who were attracted to doctors offices, clinics, hospitals, and nursing homes in search of what they viewed as an ATM."

Since their inception in 2007, Strike Force teams in the nine cities where they operate have charged more than 2,300 defendants who collectively falsely billed Medicare more than \$7 billion. Today's announcement marked the first time that districts outside Strike Force locations have participated in a national takedown; those districts accounted for 82 of the arrests this week.

Here's a look at some of the cases:

- In Miami, 73 were charged in schemes involving about \$263 million in false billings for pharmacy, home health care, and mental health services.
- In Houston and McAllen, 22 were charged in cases involving more than \$38 million. In one case, the defendant coached beneficiaries on what to tell doctors to make them appear eligible for Medicare services and then received payment for those who qualified. The defendant was paid more than \$4 million in fraudulent claims.
- In New Orleans, 11 people were charged in connection with home health care and psychotherapy schemes. In one



Attorney General Loretta Lynch is joined by HHS Secretary Sylvia Mathews Burwell (left) and FBI Director James B. Comey at a press conference on the takedown.

case, four defendants from two companies sent talking glucose monitors across the country to Medicare beneficiaries regardless of whether they were needed or requested. The companies billed Medicare \$38 million and were paid \$22 million.

"We will not stop here," said HHS Secretary Sylvia Mathews Burwell. "We will work tirelessly to prevent these programs from becoming targets and fight fraud wherever we find it."

More than 900 law enforcement officials participated in the three-day sweep. Those arrested include 46 licensed medical professionals, including 19 doctors. Since 2007, the Medicare Fraud Strike Force has prosecuted more than 200 doctors and more than 400 medical professionals.

In fiscal year 2014, DOJ and HHS health care fraud and prevention efforts recovered nearly \$3.3 billion. Over the past five years, DOJ specifically has recovered more than \$15 billion in cases involving health care fraud. The average prison sentence in Strike Force cases in fiscal year 2014 was more than four years, though some prosecutions in recent years resulted have in sentences of 50 years.

# Multi-State Chop Shop Operation Disrupted

## Criminal Enterprise Leader Among Those Convicted

In the early 1990s, a Toledo, Ohio man—Michael Wymer—was sentenced to a lengthy term in state prison for heading up an extensive truck theft and chop shop operation.

Wymer, however, apparently never learned his lesson. Upon his release from prison several years ago, he picked up where he left off, setting up another criminal enterprise to steal trucks, disassemble them in his chop shop, and sell them as scrap metal. But this time, Wymer's activities—which crossed state lines—garnered the attention of the FBI, and last month, the 56-year-old was sentenced in federal court to 27 years in prison. And Wymer's 13 co-conspirators—including his son, two brothers, and two nephews—have all either pled guilty or been convicted at trial for their roles in the illegal enterprise.

At Wymer's sentencing appearance, the federal judge ordered that all of the defendants in the case share in paying restitution to the victims of their crimes—mostly independent truck owners/operators—to the tune of nearly \$2.3 million. That figure, according to the judge, is likely a low estimate and doesn't take into account the emotional harm suffered by the victims, whose trucks were often their livelihoods.

According to the charges brought against Wymer and the others in the case, the scheme ran from at least August 2012 through February 2013. Wymer and his cohorts usually traveled outside of the Toledo area—including to Michigan and Indiana—to steal the trucks so they could avoid detection by one single jurisdiction.

Here's how the scheme worked:



**A surveillance image shows members of Michael Wymer's Ohio chop shop operation emptying scrap aluminum cargo out of a stolen trailer so the trailer could be chopped up and sold as scrap metal.**

Wymer and several others involved in the enterprise went out on the road “shopping” for semi-trucks and trailers, often at truck stops or other locations where trucks might converge that were fairly close to interstate highways. But they wouldn't hesitate to stop virtually anywhere if an opportunity presented itself.

They would usually be in Wymer's personally owned semi-truck (minus a trailer) or in a car that belonged to Wymer. If they were in the semi, they would back the truck onto the trailer they wanted and then tow it away. If in the car, one or two of the perpetrators would break into an empty semi-truck with an attached trailer, manipulate the ignition to get it started, and drive the entire vehicle onto the closest interstate highway.

In terms of the cargo these stolen trucks were carrying, Wymer preferred items that could be chopped into scrap metal—so he stole things like motorcycles, all-terrain vehicles, copper wire, spools of metal, even actual loads of scrap metal. How did he know what the trucks were hauling? By breaking into the trailers and taking a look.

Once back in Toledo with the stolen property, Wymer would take the truck to one of his two chop shop locations, where he had everything he needed—from heavy moving equipment and floor jacks to blow torches and chain saws. And he moved quickly—he could remove the parts from the truck (to sell them), and then “chop” the rest of the truck, the trailer, and the trailer's contents into scrap metal within a couple of hours. He would then load the material into one of his trucks and transport it to various businesses and/or recycling companies interested in buying scrap metal.

How did we get the evidence we needed to convict Wymer and his crew? Much of it came from video surveillance cameras, one placed by law enforcement on utility poles outside each of Wymer's chop shop locations, and several more placed by Wymer himself inside his chop shops to keep an eye on his merchandise. So we were able to see the stolen trucks and trailers being driven into these shops—and those same vehicles being taken apart by Wymer and his employees.

Because of the interstate nature of the case, there were a number of law enforcement agencies both inside and outside Ohio that played a role in the investigation. Special thanks to the Ohio State Highway Patrol—who joined our new Organized Crime Task Force shortly after the investigation—and the Ohio Bureau of Motor Vehicles for their efforts.

As for Michael Wymer, his lengthy sentence in the federal system almost guarantees that he will not get a third opportunity to break the law.



# Behind the Scenes with Operational Medics

## A Look Inside Our Washington Field Office's OpMed Program



During a training exercise, medics prepare a wounded agent for helicopter transport to a hospital. Training scenarios are meant to mimic real-world conditions, which can include hostile environments accessible only by helicopter.

The wounded man needed to be airlifted to a hospital immediately, and in the shadow of deafening helicopter blades whose wash was strong enough to knock a person over, special agents worked quickly to secure the patient to a stretcher and prepare to care for him in the close quarters of the aircraft.

Although this was only an exercise, the highly trained members of the FBI's Operational Medicine (OpMed) Program were focused on their mission—to provide care under the most stressful situations. Whether for a fellow agent engaged in a SWAT operation or a violent criminal injured during a high-risk arrest, the “medics,” as they are known, don’t distinguish between who needs treatment.

“We are on hand during tactical situations to take care of medical

emergencies,” said Special Agent Doug Mohl, who coordinates the Washington Field Office (WFO) program. “This work is great,” he explained, “because usually agents are protecting the public by putting bad guys in jail. But operational medicine personnel get to take care of people. We may meet an individual on one of the worst days of his life—or one of our fellow agents on the worst day of his career—and we render care to them and try to make sure they stay healthy.”

***“Everybody on the team is an FBI agent first.”***

There is at least one medic in each of the FBI’s 56 field offices. (Regardless of whether agents are trained as Emergency Medical Technicians—EMTs—or

paramedics, they are all referred to as medics.) They deploy with SWAT, accompany agents on high-risk arrests, and often are part of Rapid Deployment Teams that travel the world to support Bureau investigations and operations.

Because agents and critical response professionals may find themselves in harm’s way—in war zones, for example, or responding to the potential use of chemical or biological agents—the possibility of injury or illness is real, and sometimes appropriate medical facilities are not close by. That’s why OpMed personnel are highly valued and why they train to keep their skills sharp, even though it’s a collateral duty.

“Everybody on the team is an FBI agent first,” Mohl explained. “They work their cases, but when they





Members of the FBI's Operational Medicine Program are trained to provide care under the most stressful situations, such as SWAT operations and high-risk arrests. The Washington Field Office, with more than 20 special agents trained as EMTs and paramedics, has the largest "OpMed" program of any FBI office.

have a mission, they step away from their investigations, step into their role as medics, deal with the situation, and then come back to their regular duties."

Mohl, a paramedic, added that agents who are drawn to the OpMed program put in the extra time and effort because they are dedicated, "and they like helping people." The WFO team is the largest of any FBI office, with more than 20 members trained as EMTs and paramedics.

On this day at the Bureau's Quantico, Virginia training facility, the WFO team will work through a number of patient scenarios that require thoughtful assessment and quick treatment.

"We want to make this feel like real-life situations," Mohl said, so

the medics rotate through stations and are required to assess and treat someone with chest pains, a car crash victim, and an agent injured during a tactical operation, among others.

In tactical situations, Mohl said, medics have a different set of challenges than typical EMTs and paramedics. Besides the stress of being in a potentially threatening environment, they must carry all the gear they need.

"Sometimes medics won't have the support of an ambulance," he explained, "so they have to carry what they need medically in addition to what's required as an agent. Your kit might include a belt with firearms and ammunition, you may have a long gun, a ballistic vest, helmet, goggles, and hearing protection, so it can

be hard to hear. There may be a lot of distractions from a physical standpoint—lugging all that stuff around that weighs an extra 30 pounds, kneeling over a patient or sitting in the backseat of a car trying to render care."

The Washington Field Office team has a diverse background, to include past careers as flight paramedics, EMS supervisors, EMT instructors, and volunteer firefighters. Still, they all share one thing in common, Mohl said. "They are motivated to go above and beyond what is normally expected of them, to deal with pressure and stressful situations, and to be able to adapt."

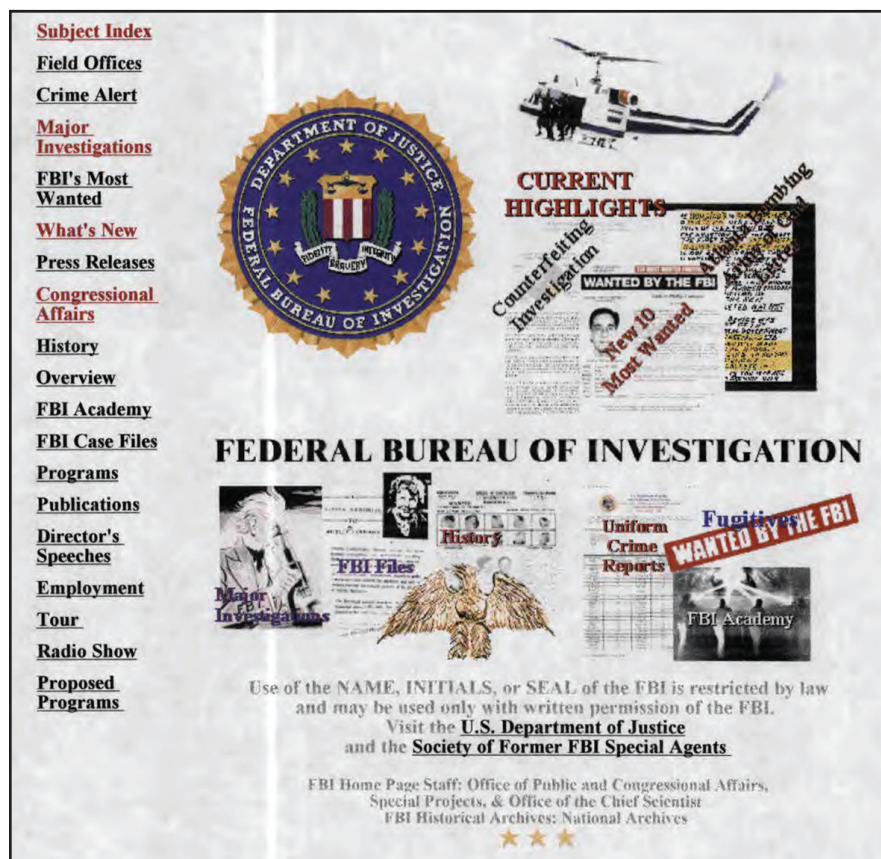


Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/opmeds](http://www.fbi.gov/opmeds).



# The FBI Website at 20

## Two Decades of Fighting Crime and Terrorism



Left: The FBI.gov homepage as it appeared in June 1997.

in social media in 2008; today, a steady stream of pictures, podcasts, and videos are broadcast on various channels, including via a specific Most Wanted Twitter feed set up three years ago. In December 2012, the Bureau built the first national electronic repository of its wanted bank robbers on a dedicated website that includes a gallery of nearly 500 searchable suspects and a map that plots robbery locations.

The collective result of all these efforts has been a rising tide of digitally driven captures. Over two decades, a total of 71 fugitives and missing persons have been located as a direct result of the FBI's web presence, an average of one every three-and-a-half months. Hundreds—if not thousands—more cases involving fugitives and missing persons have been supported by web publicity. There is no longer a need for wanted posters to be tacked to the walls of American post offices when they can be put right at the fingertips of the three billion Internet users around the world.

From its earliest days, the FBI website has sought information from the public on high-profile cases—including the search for the infamous “Unabomber” in the mid-1990s. But it was the terrorist

In the spring of 1996, a 14-year-old American living in Guatemala happened to visit the less-than-year-old FBI website, apparently out of curiosity.

To his great surprise, the teen immediately recognized a Top Ten fugitive featured on FBI.gov. It was “Uncle Bill”—a family friend and handyman who, ironically, had helped hook up the boy's computer a few weeks earlier.

In reality, Uncle Bill was Leslie Ibsen Rogge, a prolific bank robber who is believed to have pocketed an estimated \$2 million from about 30 bank heists across the United States. Rogge landed on the FBI's Ten Most Wanted Fugitives list in January 1990 and fled to Guatemala about two years later. He had been on the run more than a decade when the teen made his shocking discovery. The ensuing manhunt and media exposure

convinced Rogge to surrender to an FBI agent at the U.S. Embassy in Guatemala City on May 18, 1996.

For the Bureau, Rogge's capture was a milestone. The FBI.gov website was launched on June 30, 1995—20 years ago today—populated with digital versions of the organization's signature wanted flyers. Less than 11 months later, the site played a direct role in reeling in its first fugitive, a Top Tenner no less. Most likely, the itinerant bank robber represented the first cyberspace capture in the history of U.S. law enforcement.

Rogge's arrest served as something of a proof of concept for the FBI's use of the Internet as a crime-fighting tool. It has been full steam ahead ever since. FBI.gov now features hundreds of fugitives and missing persons in multiple categories of crime and terrorism. The Bureau dipped its first toe



**LESLIE ISBEN ROGGE**  
Former Top Ten Fugitive Leslie Ibsen Rogge was the first fugitive captured as a result of appearing on the FBI.gov website, which launched on June 30, 1995.

attacks of September 11, 2001 that by necessity propelled FBI.gov forward as an operational tool. That day, as the massive investigation got underway, the Bureau quickly stood up an electronic form to gather tips on the attacks from the public. Information came pouring in, and the tip line has been going strong ever since, now expanded to any criminal or national security investigation. This April, it logged its four millionth tip. The submissions have provided vital intelligence in terrorism and espionage cases and prevented a number of shootings and attacks on U.S. soil, including imminent threats to everyone from soldiers to schoolchildren.

*This April, FBI.gov logged its four millionth tip. The submissions have provided vital intelligence in terrorism and espionage cases and prevented a number of shootings and attacks on U.S. soil, including imminent threats to everyone from soldiers to schoolchildren.*

Increasingly in recent years, FBI.gov also has been integrated into publicity campaigns to reignite cold cases and to aid high profile probes. To support the investigation into the attacks on the U.S. Special Mission in Benghazi in September 2012, for instance, the Bureau set up a special Facebook page in Arabic seeking information from people in Libya and nearby countries.

Along with its investigative

#### FBI Web Technology Timeline

- June 30, 1995: FBI.gov website launched
- 1996: First websites for FBI field offices
- May 18, 1996: First fugitive caught as a result of FBI.gov publicity
- January 1998: Freedom of Information Act (FOIA) webpage set up
- September 11, 2001: Electronic tip line established
- February 8, 2002: First Internet-based special agent application
- October 2006: E-mail alerts started
- September 2007: FBI “widgets” launched
- May 2008: First FBI podcasts on iTunes
- November 2008: FBI Twitter site set up
- May 2009: FBI Facebook and YouTube sites established
- October 2010: National Stolen Art File goes online
- April 1, 2011: Electronic FOIA library—The Vault—established
- August 5, 2011: FBI Child ID App announced, Bureau’s first mobile application
- October 15, 2012: FBI Safe Online Surfing website established
- December 2012: Wanted Bank Robbers website launched
- April 2013: Dedicated Boston Marathon tips page set up to accept videos and images

value, FBI.gov—as well as the various other specialized Bureau websites that have emerged over the years—supports the needs of many different customers, from the researchers who pore over crime statistics to the police professionals around the world who read the regular *FBI Law Enforcement Bulletin*. Among other things, these websites enable the public to electronically read Bureau records, explore Bureau careers, and learn about cyber safety.

Over the past 20 years, the FBI’s web presences have become effective crime-fighting and customer service tools, increasingly vital to protecting the public and carrying out the Bureau’s daily work. FBI.gov has been viewed an estimated one billion times since 1995, with traffic to its more than 180,000 pages now averaging around 10 million visits a month. The Bureau’s online presence today also includes 54 social media sites or pages; the agency’s main Facebook and Twitter pages alone have a combined following of 2.2 million people, while its videos on YouTube have nearly 40 million views.

*FBI.gov has been viewed an estimated one billion times.*

Back in 1996, a single poster on what was then a sparse FBI.gov website forced an international fugitive to turn himself in. Today, thanks to the growing capabilities of the Bureau’s websites, there is less and less room for criminals and terrorists to hide.

#### Top Ten Tools of FBI.gov

People visit FBI.gov for all kinds of reasons. The following are among the features and tools used most often by the public.

1. Report Threats and Crimes
2. Find a Fugitive
3. Research Crime Statistics
4. Explore FBI Careers
5. Request a Background Check
6. Learn About Our Cases
7. Read Actual FBI Files
8. Get Educated on Scams
9. Check Sex Offender Registries
10. Subscribe and Share



# Sextortion

## Help Us Locate Additional Victims of an Online Predator



Ashley Reynolds was a happy 14-year-old who loved sports, did well in school academically and socially, and enjoyed keeping a journal she intended her “future self” to read. But what happened in the summer of 2009 was so devastating that she couldn’t bring

herself to record it in her diary—or speak about it to anyone.

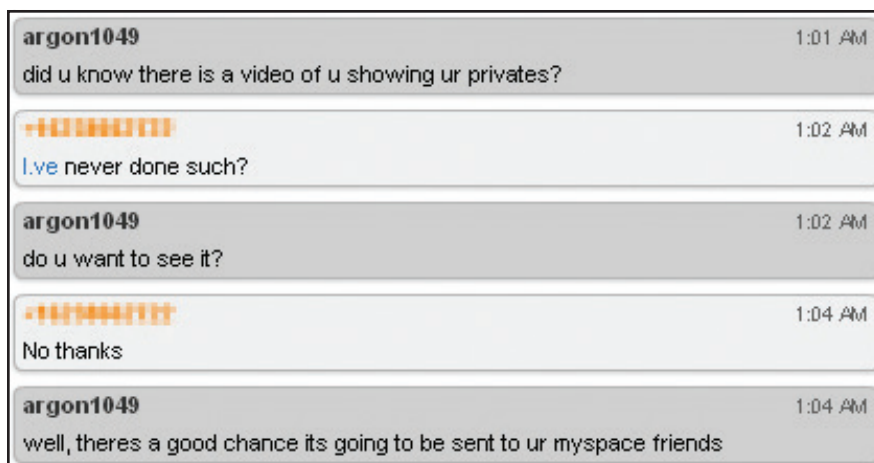
She had become the victim of sextortion, a growing Internet crime in which young girls and boys are often targeted. Her life was being turned upside down by an online predator who took

advantage of her youth and vulnerability to terrorize her by demanding that she send him sexually explicit images of herself.

After several months, Ashley’s parents discovered what was happening and contacted the National Center for Missing & Exploited Children (NCMEC). Ashley and her parents later supported the FBI investigation that led to the arrest of 26-year-old Lucas Michael Chansler, who last year pled guilty to multiple counts of child pornography production and was sent to prison for 105 years—but not before he used the Internet to victimize nearly 350 teenage girls. The majority of those youngsters have not yet been identified.

### Locations of Identified Sextortion Victims\*





Part of an online chat between Lucas Michael Chansler and one of his victims.

That's why the FBI is requesting the public's help—and why Ashley has come forward to tell her story—so that Chansler's victims can be located and will know, as Special Agent Larry Meyer said, “that this dark period of their lives is over.”

Meyer, a veteran agent in the FBI's Jacksonville Division who investigates crimes against children, explained that 109 of Chansler's victims have been identified and contacted so far, leaving approximately 250 teens “who have not had closure and who probably haven't obtained counseling and other help they might need.” He noted that Ashley is a brave person with a supportive family “and has been able to use this experience to make her stronger.” Unfortunately, that has not been the case for all the girls, some of whom have dropped out of school and tried to end their lives.

Chansler, who was studying to become a pharmacist, used multiple personas and dozens of fake screen names—such as “HELLOthere” and “goodlookingguy313”—to dupe girls from 26 U.S. states, Canada, and the United Kingdom. And he used sophisticated techniques to

keep anyone from learning his true identity.

Pretending to be 15-year-old boys—all handsome and all involved in skateboarding—he trolled popular online hangouts to strike up relationships with teenage girls. In one instance on Stickam, a now-defunct live-streaming video website, evidence seized from his computer showed four girls all exposing their breasts. “The girls are apparently having a sleepover, and Chansler contacted one of them through a random online chat,” Meyer said. “These girls thought they were having a video chat session with a 15-year-old boy that they would never see or hear from again, so they are all exposing themselves, not realizing that he is doing a screen capture and then he's coming back later—very often in a different persona—saying, ‘Hey I've got these pictures of you, and if you don't want these sent to all your Myspace friends or posted on the Internet, you are going to do all of these naked poses for me.’”

“It went from what would be relatively benign pictures to fulfilling Chansler's perverted desires,” Meyer said, adding that while adults know that a young



### Don't Become a Victim of Sextortion

Special Agent Larry Meyer and other investigators experienced in online child sexual exploitation cases offer these simple tips for young people who might think that sextortion could never happen to them:

- Whatever you are told online may not be true, which means the person you think you are talking to may not be the person you really are talking to.
- Don't send pictures to strangers. Don't post any pictures of yourself online that you wouldn't show to your grandmother. “If you only remember that,” Meyer said, “you are probably going to be safe.”
- If you are being targeted by an online predator, tell someone. If you feel you can't talk to a parent, tell a trusted teacher or counselor. You can also call the FBI, the local police, or the National Center for Missing & Exploited Children's CyberTipline.
- You might be afraid or embarrassed to talk with your parents, but most likely they will understand. “One of the common denominators in the Chansler case,” Meyer noted, “was that parents wished their daughters had told them sooner. They were very understanding and sympathetic. They realized their child was being victimized.”

person's life is only beginning in high school, “to a 13- or 14-year-old girl, thinking that all her friends or her parents might see a picture of her exposing her breasts, the fear was enough to make them comply with Chansler's demands, believing they had no better options.”

When FBI agents interviewed Chansler after his arrest, they





Ashley Reynolds, who was a victim of Lucas Michael Chansler's sextortion scheme, hopes her story helps prevent other teens from falling for similar ploys.

asked why he selected that age group. "One of the comments he made," Meyer said, "was that older girls wouldn't fall for his ploy."

Ashley fell for Chansler's ploy in late 2008 when she was 14 years old. She was contacted online by someone who claimed to be a teenage boy with embarrassing sexual pictures of her. His screen name was CaptainObvious, and he threatened to send Ashley's pictures to all her Myspace friends if she didn't send him a topless image of herself. Without considering the consequences, she sent it. She didn't think the boy knew who she was or anything else about her. Nothing more happened until the summer of 2009, when

Chansler's persona messaged again, threatening to post her topless picture on the Internet if she didn't send him more explicit images.

*"I never thought this would happen to me, but it did."*

She ignored him at first, but then he texted her on her cell phone. He knew her phone number and presumably where she lived. Somehow he must have hacked information from her social media pages. Chansler was relentless. He badgered her for pictures and continued to threaten. The thought of her reputation being ruined—and disappointing her

parents—made Ashley finally give in to her tormenter.

The next few months were a nightmare as Ashley complied with Chansler's demands. She was trapped and felt she couldn't talk to anyone. She kept thinking if she sent more pictures, the monster at the other end of the computer would finally leave her alone. But it only got worse—until the day her mother discovered the images on her computer.

"I just remember breaking down and crying, trying to get my dad not to call the police," Ashley said, "because I knew that I would end up in jail or something because I complied and I sent him the

pictures even though I didn't want to. I tried to think rationally, like this guy was threatening me. But I sent him the pictures, so that's breaking the law, isn't it? I am under age and I am sending him naked pictures of me. I didn't want to go to jail."

Still, she was relieved that she didn't have to keep her secret any longer. And her parents were supportive.

Ashley's mother did some research and contacted the NCMEC's CyberTipline. An analyst researching the case was able to tie one of the screen names used to sextort Ashley to another case in a different state and realized the predator most likely had multiple victims. Eventually, FBI and NCMEC analysts were able to pinpoint an Internet account in Florida where the threats were originating, and that information was passed to FBI agents who work closely with NCMEC in child exploitation investigations.

When investigators executed a search warrant at Chansler's Jacksonville house and examined his computer, they found thousands of images and videos of child pornography. They also found folders labeled "Done" and "Prospects" that contained detailed information about the nearly 350 teens he had extorted online.

Meyer and the Jacksonville Crimes Against Children Task Force analyzed the images of the girls to identify and locate them. One victim was located through a picture of her and her friends standing in front of a plate glass window at their school. Reflected in the glass was the name of the school, which led to her identification. Another victim



**Special Agent Larry Meyer led the FBI's investigation of Lucas Michael Chansler.**

was found through a radio station banner seen in a video hanging on her bedroom wall. The station's call letters led to a city and, eventually, to the victim. More than 250 investigators, analysts, victim specialists, child forensic interviewers, and community child advocacy centers were involved in locating and interviewing the known victims.

But approximately 250 victims are still unidentified and may have no idea that Chansler was arrested and sent to jail.

"It's important that we find these girls so that they don't have to be looking over their shoulder, wondering if this guy is still out there and is he looking for them and is he going to be coming back," Meyer explained, adding that "some of these girls, now young women, need assistance. Many probably have never told anyone what they went through."

Ashley, now 20, is doing what she can to get the word out about sextortion so that all of Chansler's victims can be identified and other girls don't make the mistakes that she made. "This ended for me," she said, but for many of Chansler's victims, "this never ended for them."

When Meyer began working crimes against children cases eight years ago, he visited freshman and sophomore high school classes to talk about Internet safety. "Now," he said, "we are going to fourth and fifth grade because kids are getting on the Internet at younger ages."

He added, "We know that youngsters don't always make sound decisions. Today, with a smartphone or digital camera, an individual can take an inappropriate picture of themselves and 10 seconds later have it sent to someone. Once that picture is gone," he said, "you lose all control over it, and what took 10 seconds can cause a lifetime of regret."

For her part, Ashley hopes that talking about what she went through will resonate with young girls. "If it hits close to home, maybe they will understand. High school girls never think it will happen to them," she said. "I never thought this would happen to me, but it did."



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/sextortion](http://www.fbi.gov/sextortion).



# Investigating Human Rights

## Reaching Out to Diaspora Communities in U.S. for War Crimes Tips



The FBI's International Human Rights Unit, working with agents in the field and partner agencies, is reaching out to diaspora communities in the U.S. for leads on war criminals who may be residing among them.

Five years ago, nearly a dozen former soldiers who served during the Bosnian civil war in the early '90s before settling in Arizona were sentenced for lying on their applications for refugee status when they came to the U.S. Last year, a Bosnian-born Minnesota man was arrested on fraud charges for not disclosing crimes—including murder, kidnapping, and robbery—he allegedly committed during his military service in Bosnia-Herzegovina. In January, a Bosnian-born Vermont man was found guilty of lying to get into the U.S. and obtain his naturalized citizenship.

These cases illustrate efforts across multiple agencies and international borders to hold accountable any individuals who committed war crimes or atrocities overseas before entering and settling in the United States. And Bosnian war

criminals represent just a sampling of the subjects being sought. The U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) is pursuing more than 1,900 leads and cases on individuals from about 96 countries. The FBI, which works alongside HSI and special prosecutors at the Human Rights Violators and War Crimes Center in Northern Virginia, has pending investigations in nearly a third of our 56 field offices.

***The FBI is seeking tips on the whereabouts of suspected war criminals and human rights violators.***

Managing the FBI's role in identifying, locating, and investigating these cases is the Bureau's International Human

Rights Unit (IHRU), which works closely with partner intelligence agencies and the Department of State to identify subjects and gather leads. Agents in the unit then coordinate the FBI's approach in the field—whether it's collecting intelligence, developing sources, or just meeting leaders in diaspora communities to make them aware that the FBI is seeking tips on the whereabouts of suspected war criminals and human rights violators.

"We are asking those communities, 'If you know somebody or if you have heard of somebody who has done those things, let us know and then we'll go from there,'" said Thomas Bishop, head of the IHRU. "I think in a lot of these communities, people know someone who was involved with something—or they hear about somebody being involved—but

they may not know what to do with it. All we need is a tip so we can see if there's anything to it."

The FBI has had an expanding role investigating human rights crimes since 1988, when Congress added genocide to the U.S. criminal code. Torture was included in the code in 1994 and war crimes in 1996. The most recent addition, in 2008, was the recruitment of child soldiers—an offense exemplified at the time by fugitive Ugandan warlord Joseph Kony, who famously recruited children into his notorious Lord's Resistance Army.

Following the Presidential Study Directive on Mass Atrocities in 2011, the FBI formalized an international human rights program to leverage its intelligence capabilities and vast network of field agents and analysts. The genocide and war crimes program, as it was then called, was originally part of the FBI's Counterterrorism Division, but last fall it was reorganized under the Criminal Division's Civil Rights Program and given its current name. Jeffrey Sallet, head of the Bureau's Public Corruption/Civil Rights Section, which includes IHRU, said the shift creates a one-stop shop of experts on human rights and public corruption matters, which often go hand-in-hand.

"Corruption leads to lack of confidence in government," he said. "Lack of confidence in government leads to failed states. And failed states lead to terror and human rights abuses. The people who are kleptocrats and robbing their countries are often the same people who are committing these abuses."

Agents in the IHRU have territories they manage—Africa,

**Investigating Human Rights Violations**

The FBI, through its International Human Rights Unit, plays a vital role in the U.S. government's coordinated efforts to identify, locate, investigate, and prosecute perpetrators of genocide, war crimes, and other related mass atrocities.

You can help. If you believe you may have information concerning a specific incident of genocide, war crimes or other mass atrocities or related violations, please submit that information to us at [tips.fbi.gov](https://tips.fbi.gov) or contact your local FBI office, domestically or internationally.

#### International Human Rights Unit webpage

Latin America, for example—and work directly with agents in the field when they need a lead covered.

*"...The people who are kleptocrats and robbing their countries are often the same people who are committing these abuses."*

"We're going to go out to the field office and say, 'We have a file, we have these requirements, will you go out and talk to your sources and collect this information?'" said Vanya Voivedich, a special agent in the unit. When the information comes back, it is shared and analyzed to either build a case or close a lead.

In some cases, when crimes occurred before the U.S. war crimes statutes were in place, subjects can still be prosecuted on lesser violations. Subjects who lied about their refugee status are subject to deportation to their home countries. One of the defendants in the Phoenix case in 2010, Mladen Blagojevic, was

ultimately sent back to Bosnia-Herzegovina, where he was tried and sentenced to seven years in prison for crimes against humanity.

Pointing to the 20-year anniversary of the July 1995 genocide in the Bosnian town of Srebrenica, in which around 8,000 men and boys were killed or taken prisoner, the FBI is renewing its plea for tips to bring to justice anyone involved in human rights violations.

"People in diaspora communities know each other," said Voivedich, "they'll know if someone in their community committed atrocities and are now here enjoying the benefits of starting a new life. And they see how that may not be fair."

#### Contact the FBI

The FBI seeks information from diaspora members, refugees, and asylum seekers here in the U.S. with knowledge of human rights violations committed abroad.

If you have any information about perpetrators of genocide, war crimes, or other related mass atrocities, please submit it to us at [tips.fbi.gov](https://tips.fbi.gov) or contact your local FBI office, domestically or internationally.



# Cyber Criminal Forum Taken Down

## Members Arrested in 20 Countries

It was, in effect, a one-stop, high-volume shopping venue for some of the world's most prolific cyber criminals. Called Darkode, this underground, password-protected, online forum was a meeting place for those interested in buying, selling, and trading malware, botnets, stolen personally identifiable information, credit card information, hacked server credentials, and other pieces of data and software that facilitated complex cyber crimes all over the globe.

Unbeknownst to the operators of this invitation-only, English-speaking criminal forum, though, the FBI had infiltrated this communication platform at the highest levels and began collecting evidence and intelligence on Darkode members.

And today, the Department of Justice and the FBI—with the assistance of our partners in 19 countries around the world—announced the results of Operation Shrouded Horizon, a multi-agency investigation into the Darkode forum. Among those results were charges, arrests, and searches involving 70 Darkode members and associates around the world; U.S. indictments against 12 individuals associated with the forum, including its administrator; the serving of several search warrants in the U.S.; and the Bureau's seizure of Darkode's domain and servers.

Said FBI Deputy Director Mark Giuliano, "Cyber criminals should not have a safe haven to shop for the tools of their trade, and Operation Shrouded Horizon shows we will do all we can to disrupt their unlawful activities."



During the investigation, the Bureau focused primarily on the Darkode members responsible for developing, distributing, facilitating, and supporting the most egregious and complex cyber criminal schemes targeting victims and financial systems around the world, including in the United States.

The Darkode forum, which had between 250-300 members, operated very carefully—not just anyone could join. Ever fearful of compromise by law enforcement, Darkode administrators made sure prospective members were heavily vetted.

Similar to practices used by the Mafia, a potential candidate for forum membership had to be sponsored by an existing member and sent a formal invitation to join. In response, the candidate had to post an online introduction—basically, a resume—highlighting the individual's past criminal activity, particular cyber skills, and potential contributions to the forum. The forum's active members decided whether to approve applications.

Once in the forum, members—in addition to buying and selling criminal cyber products and services—used it to exchange ideas, knowledge, and advice on any number of cyber-related fraud schemes and other illegal activities.

Left: This message was displayed on the Darkode homepage after the FBI seized its web domain and servers.

It was almost like think tank for cyber criminals.

What's the significance of this case, believed to be the largest-ever coordinated law enforcement effort directed at an online cyber criminal forum? In addition to shutting down a major resource for cyber criminals, law enforcement infiltrated a closed criminal forum—no easy task—to obtain the intelligence and evidence needed to identify and prosecute these criminals. And this action paid off with a treasure trove of information that ultimately led to the dismantlement of the forum and law enforcement actions against dozens of its worst criminal members around the world.

The case was led by the FBI's Pittsburgh Field Office, with assistance from our offices in Washington, San Diego, and a number of others around the country. But it wouldn't have happened without the support of Europol and other partners in 19 countries. And in addition to the FBI obtaining enough evidence for search warrants and indictments in the U.S., we shared information with our foreign partners to help them make their own cases against the Darkode perpetrators residing in their jurisdictions.

Operation Shrouded Horizon is a prime example of why the most effective way to combat cyber crime—which operates globally—is a law enforcement response that also transcends national borders.

# International Law Enforcement Training

## Celebrating 20 Years of Partnership and Excellence

American law enforcement celebrated a milestone today in Budapest, Hungary: the 20th anniversary of an international training program whose success continues to prove that despite diverse cultures, politics, and religions, police officers everywhere share many more similarities than differences.

The FBI was instrumental in establishing the International Law Enforcement Academy (ILEA) in Budapest in 1995, and since that time, instructors from a variety of U.S. federal agencies have provided expert training to more than 21,000 law enforcement officers from more than 85 countries.

Just as importantly, the program encourages officers of different nationalities to build lasting professional relationships to better fight crimes that increasingly spill across borders. The concept has worked so well that other ILEAs—all funded and run by the U.S. Department of State—have been opened in Thailand, Botswana, El Salvador, and America.



**FBI Special Agent John Terpinas, director of the International Law Enforcement Training Academy (ILEA) in Budapest, Hungary, speaks at a July 17, 2015 event there celebrating the organization's 20th anniversary and the graduation of its 100th core class.**

"It's one of the program's biggest strengths," said FBI Special Agent John Terpinas, director of ILEA Budapest. "Beyond the classroom instruction, we help to build relationships, and those relationships—that ILEA network—have opened a lot of doors over the last 20 years that might otherwise have been closed."

"From the perspective of the U.S. government and particularly the FBI, I can't emphasize enough how important ILEA is for the entire international law enforcement

community," noted Robert Anderson, Jr., executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch. Anderson was on hand at events in Budapest to celebrate the anniversary, along with foreign dignitaries and U.S. Ambassador to Hungary Colleen Bell.

Also in attendance was former FBI Director Louis Freeh, who in 1994—only a few years after the fall of the Berlin Wall—led a U.S. delegation to meet with representatives from 11 nations



**The FBI's John Terpinas is director of ILEA Budapest.**



**Lt. Colonel Hajni Gósi has been with ILEA Budapest since 1997.**



**Colonel István Farkas oversees Hungarian staff at ILEA Budapest.**



**János and Márk Wodala are a father-son interpreting team.**



**Máté Németh is a Hungarian police detective and ILEA student.**



**Retired FBI Special Agent Skip Stites taught tactical classes.**





ILEA was established in Budapest, Hungary in 1995. Right: Dignitaries, including then-FBI Director Louis Freeh and former U.S. Attorney Janet Reno, congratulated the first graduating class, which consisted of 33 students from Hungary, Poland, and the Czech Republic.



ILEA Budapest's instruction covers various disciplines including counterfeiting (center), and forensics.

in Russia, Eastern Europe, and Central Europe. The mission was to determine if new joint programs with these emerging democracies could be created to fight the growing threat of transnational crime.

The former Soviet countries had little experience with Western methods of policing and operating a criminal justice system under the rule of law, and they asked Freeh for FBI training.

"Many newly appointed police chiefs were democratically minded but had little previous police experience and no experience in Western law enforcement leadership and methodology," said Miles Burden, a retired FBI special agent and former ILEA director who was on the 1994 trip. "They had no experience in things as basic as serving a warrant. You couldn't wave a magic wand and

change that without extensive training."

*"No country by itself, no matter how strong it may be, can face all of this crime alone and hope to succeed."*

A little more than a year later, ILEA Budapest was offering instruction to its first class, and in the spring of 1996, Freeh was there for the first graduation ceremony. "The reasons for the academy's success are apparent to anyone who looks in realistic ways at the world around us," he said at the time. "Crime of all kinds has grown to alarming levels on an international scale. No country by itself, no matter how strong it may be, can face all of this crime alone and hope to succeed."

While most of the Eastern European countries that participate in ILEA Budapest today are no longer emerging democracies, the need for joint training and partnerships is as important as ever.

"ILEA is more relevant now in the world that we live, particularly with law enforcement challenges, than when it was established 20 years ago," Freeh said this week, adding that he was "extremely proud" of what the program has accomplished and the dividends it is paying. Early ILEA participants, for example, have now assumed leadership roles in their organizations.

"Some of our students have risen all the way to the ministerial level in their governments," Terpinas explained. "We hope that their ILEA experience will help them influence their government's policy and decision making toward good





Left: Fitness at ILEA Budapest. Center and right: Firearms, tactics, and street survival skills.



Left: Sándor Pintér, the Hungarian Minister of the Interior. Center: ILEA Budapest core countries. Right: The U.S. Department of State's William R. Brownfield, and the FBI's Robert Anderson, Jr.

governance and shared values that promote democracy.”

ILEA Budapest owes much of its success to the Hungarian government that hosts the academy and the Hungarian staff who take care of the day-to-day operations—tending to students who speak different languages and may have never traveled across their own border or met an American law enforcement officer before.

“We are really lucky here in ILEA Budapest because we have an outstanding relationship with our Hungarian partners,” Terpinas said. “The staff here is spectacular. Some have been here since the day the door opened.”

Police Colonel István Farkas, who oversees the Hungarian staff at ILEA Budapest, explained that the Americans who serve as director and deputy director of the academy

usually rotate every three years, while the Hungarian staff remains constant. “What makes this academy function at high quality is that its staff has been almost the same during the course of all these years,” Farkas said through an interpreter.

*“Our classrooms are like a mini United Nations.”*

Farkas, who has been a senior leader at ILEA Budapest for 16 years, added that the U.S. government takes the international training program very seriously. “The American law enforcement professionals are not conducting a marketing activity here,” he said. “What they do is they transfer true knowledge.”

ILEA’s core course of instruction—based on the FBI’s National Academy program for U.S. law

enforcement personnel—is a seven-week program with blocks of instruction in various disciplines. Each class consists of about 50 mid-career officers from three or four different countries.

FBI instructors teach blocks on public corruption, counterterrorism, and tactics, while the U.S. Secret Service teaches about counterfeiting, and the Drug Enforcement Agency teaches about drug trafficking. “Everybody comes and teaches their expertise,” Terpinas said. The instructors are among U.S. law enforcement’s most experienced members.

In addition to the classroom and tactical instruction, students are encouraged to exercise and are required to participate in a variety of team-building activities—which help them form bonds intended to last a lifetime.





ILEA Budapest students who speak different languages wear headsets and receive simultaneous translations.

Located in a Ministry of Interior facility consisting of historic buildings that have been refurbished with state of the art equipment, ILEA Budapest overcomes the language barrier for students through the use of seasoned interpreters.

“Our classrooms are like a mini United Nations,” Terpinas said. “The students are all wearing headsets, and we can translate up to four languages simultaneously. So the instruction is in English, the materials that the students are looking at on their laptops are in their language, and then they are receiving the instruction, simultaneously, in their language from our interpreters.”

János Wodala, a longtime ILEA interpreter, likened his role to a soccer referee. “If it’s a good game,” he said, “you don’t even notice that the referee is on the field. So if interpretation goes well, and if it goes smoothly, you don’t even notice that there’s an interpreter.”

Máté Németh, a Hungarian police detective who was part of the 100th core class that graduated today to coincide with the 20th anniversary, spent the past seven weeks with fellow Hungarian officers and classmates from Macedonia and Bulgaria. Prior to his ILEA experience, he had never encountered police officers from those countries.

***“The criminals don’t stop at our borders, so we shouldn’t stop there either.”***

“I never met Macedonians or Bulgarians,” he said, “not on the professional level. So it was a really good time to get to know some colleagues from the surrounding and neighboring countries.” He added, “The biggest point of the whole ILEA is networking—getting to know these people. Because the criminals don’t stop at our borders, so we shouldn’t stop there either.”



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/ilea20](http://www.fbi.gov/ilea20).

# Financial Fraud

## The Hair Show That Never Was

Tamira Fonville's job might be described as "recruiter." For a time, she profited substantially by enlisting college-age women to participate in a hair show. The problem was, there never was any show, and everything about Fonville's line of work was a fraud.

She and her partner—both of whom are now in prison—regularly traveled the Interstate 95 corridor from New York to Washington, D.C., visiting shopping malls and other places where young women were known to spend time.

Using a series of phony names, Fonville would interest the women in the hair show, offering to pay for their services. But to pay them, she said, she needed their debit card numbers and access to their accounts.

With that access, she would not simply clean out their accounts. Instead, her partner and mastermind of the scam, Ricardo Falana, would deposit bogus checks into the legitimate accounts, and then immediately begin withdrawing funds before the bank realized the fraud.

"It was a crazy, hit or miss scheme," said Special Agent Sean Norman, who investigated the case from the FBI's Philadelphia Division. "But they did it at such a high volume that they made a lot of money for several years. There was approximately \$600,000 in actual losses to banks and other financial institutions."

On a typical recruiting trip, Fonville might talk with 20 or 30 women and would follow up with text messages using disposable phones whose numbers could not be traced. If she ended up with three or four willing participants, that was enough.



**Two criminals were sentenced for a scheme that involved enlisting young women at shopping malls and other places to participate in a "hair show," gaining access to their bank accounts, depositing phony checks in the accounts, and withdrawing funds before the banks realized the fraud.**

"Some took the hair show bait and handed over their debit cards and PINs," Norman said. "Others who were skeptical got a different pitch," he explained. "They were told: 'I can make money appear in your account. You will get some money, I will get some money, and the bank won't lose anything.'"

With access to legitimate accounts not tied to him, Falana deposited forged checks of up to \$10,000 and then withdrew money before the bank realized the checks were bad. Many of the victims were coached to tell bank investigators that their debit cards had been stolen and their PINs were written on the cards.

"The majority of the account holders knew they were doing something fraudulent," Norman said. "They thought they were going to get something out of it, but they got nothing."

For a time, the money rolled in, and Fonville "got addicted to the lifestyle," Norman said. According to court documents, between 2008 and 2013, Fonville personally benefited from the scheme to the tune of more than \$230,000. She used some of the proceeds to pay

for plastic surgery, the car loan on her \$30,000 Chevrolet Camaro, and the \$2,100 monthly rent on her New York apartment. She would later tell investigators she viewed the scam as a career.

Fonville also fraudulently obtained food stamps, Medicaid, and benefits from a New York child care program, and she received deferments on almost \$100,000 in student loans because she claimed she had no income. But then she lied on her car loan application, stating she was an employee of Mesa Airlines and had a salary of \$65,000 per year.

Eventually, some of the women whose accounts had been used came forward and told the truth. Norman was able to trace withdrawn funds to Fonville and Falana, and Falana was identified on surveillance video depositing what turned out to be bogus checks. Norman also used E-ZPass toll receipts to link the pair's recruiting trips to account holders and subsequent fraudulent transactions on their accounts.

"After the pieces all fit together," said Norman, who is a certified public account and specializes in financial fraud investigations, "their actions were highly predictable."

Fonville was arrested in August 2014. She pled guilty the following month to conspiracy to commit bank fraud and three counts of bank fraud and was sentenced in April to 15 months in prison. Falana pled guilty to similar bank fraud charges in October 2014 and in February received an 80-month sentence.

In the end, Norman said, "they blew all the money and had nothing to show for it."



# Economic Espionage

## FBI Launches Nationwide Awareness Campaign



Left: Based on an actual case, *The Company Man: Protecting America's Secrets* is part of a nationwide FBI campaign to raise awareness of the economic espionage threat.

is immune to the threat. Any company with a proprietary product, process, or idea can be a target; any unprotected trade secret is ripe for the taking by those who wish to illegally obtain innovations to increase their market share at a victim company's expense.

To raise awareness of the issue, the FBI, in collaboration with the National Counterintelligence and Security Center, has launched a nationwide campaign and released a short film aimed at educating businesses, industry leaders, and anyone with a trade secret about the threat and how they can help mitigate it. Based on an actual case, *The Company Man: Protecting America's Secrets* illustrates how one U.S. company was targeted by foreign actors and how that company worked with the FBI to resolve the problem and bring the perpetrators to justice.

The Bureau has provided more than 1,300 in-person briefings on the economic espionage threat to

Industries in the United States spend more on research and development than any other country in the world. The amount of effort and resources put into developing a unique product or process that can provide an edge in the business world is not unsubstantial. But what happens if someone comes in and steals that edge—a company's trade secrets—for the benefit of a foreign country? The damages could severely undermine the victim company and include lost revenue, lost employment, damaged reputation, lost investment for research and development, interruption in

production—it could even result in the company going out of business.

It's called economic espionage, and it's a problem that costs the American economy billions of dollars annually and puts our national security at risk. While it is not a new threat, it is a growing one, and the theft attempts by our foreign competitors and adversaries are becoming more brazen and more varied in their approach.

Historically, economic espionage has been leveled mainly at defense-related and high-tech industries. But recent FBI cases have shown that no industry, large or small,

### Defining the Crime

Theft of trade secrets occurs when someone knowingly steals or misappropriates a trade secret for the economic benefit of anyone other than the owner.

Similarly, economic espionage occurs when a trade secret is stolen for the benefit of a foreign government, foreign instrumentality, or foreign agent.

Proving the foreign nexus in court is difficult, and cases that start out as economic espionage often end up prosecuted as theft of trade secrets. Both crimes are covered by the Economic Espionage Act of 1996, Title 18, Sections 1831 and 1832 of the U.S. Code.

## Case Examples

- In May 2015, two Chinese professors were among six defendants charged 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 universities and companies controlled by the People's Republic of China (PRC).
- In January 2015, a computer science engineer was sentenced for stealing sensitive trade secrets from a trading firm in New Jersey and a Chicago-based financial firm.
- In July 2014, a California man was sentenced to 15 years in prison on multiple economic espionage-related charges in connection with his theft of trade secrets from DuPont regarding its chloride-route titanium dioxide (TiO<sub>2</sub>) production technology and the subsequent selling of that information to state-owned companies of the PRC.
- In May 2014, five Chinese military hackers were indicted on charges of computer hacking, economic espionage, and other offenses directed at six victims in the U.S. nuclear power, metals, and solar products industries.
- In March 2013, a New Jersey-based defense contractor was sentenced for theft of trade secrets and exporting sensitive U.S. military technology to the PRC.
- In December 2011, a Massachusetts man was sentenced on a charge of foreign economic espionage for providing trade secrets to an undercover federal agent posing as an Israeli intelligence officer.
- In February 2010, a former Boeing engineer was sentenced to nearly 16 years in prison for stealing aerospace secrets for the benefit of the PRC. This was the first economic espionage trial in U.S. history.

companies and industry leaders over the past year, using *The Company Man* as a training tool. But through this campaign, the FBI hopes to expand the scope of the audience to include a wider range of industry representatives, trade associations, and smaller companies and encourage them to come forward if they suspect they are a victim of economic espionage.

Understandably, companies are often hesitant to reach out for help when faced with a potential threat of this nature, usually because they don't want to risk their trade secrets being disclosed in court or compromised in any

way. But the FBI will do all it can to minimize business disruption and safeguard privacy and data during its investigation and will seek protective orders to preserve trade secrets and business confidentiality whenever possible. The Department of Justice also has a variety of protections in place to ensure that sensitive information is protected throughout any criminal prosecution.

Each of the FBI's 56 field offices has a strategic partnership coordinator (SPC) whose role is to proactively develop relationships with local companies, trade groups, industry leaders, and others so that

## Protect Your Trade Secrets

Any company that has invested time and resources into developing a product or idea needs to protect it. The FBI recommends the following methods for economic protection:

- Recognize the threat.
- Identify and value trade secrets.
- Implement a definable plan for safeguarding trade secrets.
- Secure physical trade secrets and limit access to trade secrets.
- Provide ongoing security training to employees.
- Develop an insider threat program.
- Proactively report suspicious incidents to the FBI before your proprietary information is irreversibly compromised.

if an incident occurs, a liaison has already been established. To report suspected economic espionage-related activity, please contact the SPC at your local FBI field office or submit a tip at [tips.fbi.gov](https://tips.fbi.gov).

**Below: The targeted company's corporate attorney and the FBI's lead investigator in the real-life version of *The Company Man* share their perspectives on the case, and corporate executives discuss the importance of protecting trade secrets and how their collaboration with the FBI has helped them in that endeavor in videos on our website.**



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/thecompanyman](https://www.fbi.gov/thecompanyman).



Corporate Attorney  
at Targeted Company



FBI Special Agent  
Jeremiah Crabtree



Ed Montooth,  
DuPont Corporation



Bob Trono,  
Lockheed Martin Corporation



Andy Ubel,  
Valspar Corporation



# International Parental Kidnapping Case

## Partnerships, Publicity Key to 9-Year-Old's Rescue



International parental kidnapper Jeff Hanson's boat, the *Draco*, is seen at a dry dock on the South Pacific island of Niue, where Hanson was located with his 9-year-old son in October 2014.

When 9-year-old Billy Hanson didn't return to Pennsylvania after spending the summer with his father in Seattle, the boy's mother called her local police department, setting in motion an international kidnapping investigation that led FBI agents halfway around the world to a tiny island in the South Pacific.

What would eventually bring the case to a successful conclusion was the extraordinary collaboration between local, federal, and international law enforcement and other agencies. But on that September day in 2014 when Billy was not on the flight he was supposed to be on, his mother "was obviously very concerned," said Special Agent Carolyn Woodbury, who led the investigation from the FBI's Seattle Division.

Johanna Hanson had agreed to let her son spend that July and August living with his father, Jeff Hanson, aboard a 30-foot sailboat named the *Draco*. But after Billy arrived in Washington, she began receiving text messages from her estranged husband suggesting that Billy would not be returning in the fall—a clear violation of their court-approved custody agreement.

Johanna called the Hazelton Pennsylvania Police Department, who, in turn, contacted the Port of Seattle Police Department. In August, a welfare check was conducted, which showed that Billy and his father were on the boat in Seattle, and all seemed to be well. A week later, however, the airplane ticket Billy's grandfather had purchased for his return to the East Coast was never used—and the *Draco* was nowhere to be found.

The FBI-led Seattle Safe Streets Task Force, which includes the Seattle Police Department and other law enforcement agencies, was called for assistance. Task force members who went to the marina and elsewhere to conduct interviews learned that 46-year-old Jeff Hanson had given away some of his personal belongings, that he had previously sailed the *Draco* around the world, and—most significantly—that he had a six-day head start on investigators. In other words, he was likely on the open sea and could be headed anywhere. Investigators also learned another troubling fact, Woodbury said: "We were told that Billy didn't know how to swim."

On September 12, 2014, a federal warrant was issued for Jeff Hanson, and Woodbury and task force members worked quickly

## Parental Kidnapping Case Leads to South Pacific Island



to “get the word out” about the kidnapping. FBI offices up and down the West Coast were alerted, along with the National Center for Missing & Exploited Children. The Coast Guard and U.S. Navy were notified, and hourly announcements about the kidnapping were made on maritime radio channels. In addition, the FBI’s investigative publicity team distributed posters online and on social media networks showing pictures of Billy, his father, and the *Draco*.

“Our investigation suggested that Jeff Hanson would likely sail either to Mexico, South America, or the South Pacific,” Woodbury said. The FBI’s legal attaché

offices—known as legats—were contacted, and in Australia, Legat Canberra disseminated fliers and other information to the Pacific Transnational Crime Coordination Centre, an organization of police, customs and immigrations, and other agencies whose goal is to gather and share intelligence to stop transnational crime in the South Pacific. Meanwhile, news reports about Billy’s kidnapping were being broadcast everywhere.

On October 29, 2014, Legat Canberra reported that Billy and his father had been seen on the remote island nation of Niue, located about 1,500 miles northeast of New Zealand. The island has fewer than 1,200 residents, but

a woman recognized Billy and his father from news reports and contacted the local chief of police.

Jeff Hanson was detained on immigration charges, and FBI agents from Seattle began the long trip to Niue, which is said to be one of the least visited places on the planet. There are only two flights on and off the island per week.

“The irony for Jeff Hanson,” said Woodbury, “was that he was immediately recognized in one of the most remote places in the world. For law enforcement,” she added, “it illustrates that collaboration and asking for the public’s help were the absolute keys to solving this case.” Woodbury had particular praise for the international assistance provided by the Niue Police Department, the New Zealand Police, and New Zealand Customs Service.

After his harrowing odyssey, Billy was reunited with his mother. “This was no carefree adventure for him,” Woodbury explained. “It was a traumatic experience.” Investigators learned that shortly after the *Draco* left Seattle, the dinghy that carried most of the food and water for the trip was lost at sea. By the time Billy and his father reached Niue after 60 days aboard the *Draco*, the 9-year-old had lost 30 pounds.

On November 11, Jeff Hanson appeared in federal court in Seattle to face international kidnapping charges. He pled guilty in March 2015 and was sentenced last week to time served, which was about seven months in prison. As for the *Draco*, which was Hanson’s residence, it remains in Niue in dry dock—some 5,500 miles from Seattle—accumulating dock fees.



# Sexual Predator Sentenced to 29 Years

## Targeted Young Victims Through Social Media

Social media is a great vehicle for keeping up with friends and family, networking with colleagues, and sharing common interests with others—and it's an especially popular way for young people to communicate with one another. But, like a car that's stolen by a bank robber to be used as a getaway vehicle, social media accounts can be hijacked by criminals and others for nefarious purposes. And it's often a young victim at the other end of the computer.

Which is why parents need to be aware of what could happen if their child unknowingly comes across someone on social media who poses a threat—and should talk to their kids about it. (See sidebar.)

Case in point: a 23-year-old California man who was recently sentenced to 29 years in federal prison for attempting to produce child pornography and enticing a minor. Jordan James Kirby used Facebook to solicit juvenile girls (as well as women) for sexually explicit photos, which he would then use to extort the victims for additional pictures and/or for sex acts with him.

Kirby, who lived in Paradise, California, created several bogus Facebook profiles through which he contacted hundreds of victims, many of whom were minor females. He would sometimes claim to be an agent for a modeling company and, after complimenting them on their looks, would offer the girls thousands of dollars for photos of themselves in various stages of undress. To tempt them, he posted pictures of himself holding large amounts of cash and photos of money spread out on top of his computer. Unfortunately, some of the girls he contacted were either

duped by Kirby or enticed by the money and ultimately sent him the photos he requested.

Of course, once Kirby got the photos, he never sent the money. Instead, he would up the ante—threatening to send the photos to the girls' parents or release them on the Internet unless they sent him yet more pictures, or, in some cases, met up with him for sex acts.

Kirby's illicit activities became known when the parents of one of his victims—after discovering information on a home computer—contacted the FBI's Chico Resident Agency out of our Sacramento Field Office. Our case agent then contacted a detective with the Paradise Police Department for assistance with identifying local suspects. After the execution of several search warrants on Internet service providers, investigators identified and arrested Kirby in May 2014 on state criminal charges. In the meantime, the federal case was being built against him.

This joint investigation made good use of an FBI child forensic interviewer, the FBI's Computer Analysis Response Team, and the Paradise Police Department's familiarity with the town's young people.

Earlier this year, Kirby pled guilty in federal court to six criminal counts involving victims between the ages of 10 and 15. And this past May, he was sentenced to 29 years in prison.

A key aspect of the case, according to the FBI agent who worked it, was the willingness of that one victim's parents to immediately come forward to the FBI with their concerns—and computer devices, potentially containing evidence—when they suspected their daughter may have been victimized. Their action not only led to the eventual identification of Kirby, which protected their daughter from further contact with him, but also protected an unknown number of young girls who could have been victimized by him in the future.

### Help Protect Your Kids from Online Sexual Predators

In addition to talking to your kids about the dangers of being sexually exploited online and offline, here are some concrete ways you can help them protect themselves on social media:

- Make sure the privacy settings on your kids' social media accounts are high, but also keep in mind that information can inadvertently be leaked by friends and family, so remind kids they should still be careful about posting certain information about themselves—like street address, phone number, Social Security number, etc.
- Remind your kids they should post only what they're comfortable with others seeing. Encourage them to think about the language they use online and to think before posting pictures and videos. And remind them that once they post something, they can't take it back.
- Be aware of who your kids' online friends are, and advise them to accept friend requests only from people they know personally.
- Encourage your kids to tell you if they feel threatened by someone or uncomfortable because of something online.
- Report inappropriate activity to the website or to law enforcement.
- Know that teens are not always honest about what they are doing online. Some will let their parents "friend" them, for example, but will then establish another space online that is hidden from their parents.



# Cold Case Investigation

## Solving a Decades-Old Mystery



Two decades after the murder of 6-year-old Michael Hughes, the FBI's Evidence Response Team and anthropologists from the University of Oklahoma searched an area near the Oklahoma-Texas border where Franklin Delano Floyd said he had dumped the boy's body after shooting him twice in the back of the head.

Tonya Hughes was just shy of her 21st birthday on a spring day in 1990 when she was struck by a hit-and-run driver in Oklahoma City. She died five days later, but the investigation into her suspicious death led to a mystery—and a murder—that took decades to fully unravel.

That's because Tonya Hughes was not who anyone thought she was—and neither was her husband, Clarence Hughes, who now sits on death row in a Florida prison.

"The FBI has been chipping away at this one," said Special Agent Scott Lobb, who began working the cold case investigation in 2013 out of the Bureau's Oklahoma City Division. "There were a lot of peculiar twists to this case."

Tonya left behind a child, Michael Hughes. Her husband claimed he was Michael's biological father, but

shortly after Tonya died, Clarence gave Michael to Oklahoma state welfare officials and promptly disappeared. "He knew the truth would come out," Lobb said, "and so he fled."

The truth—discovered during the hit-and-run investigation—was that Clarence Hughes was actually Franklin Delano Floyd, a federal fugitive from Georgia wanted since 1973.

Floyd was arrested in Georgia two months later and sent back to prison to serve the rest of his sentence. A blood test revealed that he was not Michael's biological father. That fact apparently didn't matter to Floyd, because when he got out of prison in 1993, he was determined to get custody of Michael. And he did—by kidnapping the 6-year-old from elementary school on September 12, 1994.

When authorities caught up with him in Kentucky two months later, Michael was nowhere to be found, and Floyd would not say what happened to the boy. Floyd was later found guilty of a federal kidnapping charge and sent to prison.

During the kidnapping investigation, photos were found taped to the gas tank of Floyd's pickup truck that showed a young woman who appeared to be bound and beaten. Years later, the woman—Cheryl Ann Comesso—was identified and matched to remains that had previously been discovered near a freeway on-ramp near Tampa, Florida. Floyd was charged with her 1989 murder, convicted, and sentenced to death in 2002.

The investigation into Michael's kidnapping also determined that Tonya Hughes, too, had been



kidnapped by Floyd—sometime between 1973 and August 1975—and when he surfaced in Oklahoma City, he began introducing his future wife as his daughter.

In 2013, the FBI and the National Center for Missing & Exploited Children conducted a cold case review of the Hughes kidnapping and reopened the investigation. A year later, Lobb and Special Agent Nate Furr spent several days interviewing Floyd in prison regarding Tonya and Michael Hughes.

***“We were able to find her birth parents and give them some closure about their daughter.”***

The death row inmate was generally uncooperative, Lobb said, but during the course of many hours of conversation, he told the agents that in 1974, under the name Brandon C. Williams, he married a woman in North Carolina who had three daughters, and the new family made its way to Texas. He identified the oldest daughter as Suzanne Marie Sevakis, born September 6, 1969, in Michigan. Floyd said that after the mother was jailed for minor charges in Dallas, he took Suzanne and moved to Oklahoma City, dropping the other two daughters at a children’s home.

Lobb later confirmed the marriage through court records, and, using DNA samples, concluded that Tonya Hughes was indeed Suzanne Marie Sevakis. It had taken 24 years to learn her true identity. “We were able to find her birth parents and give them some closure about their daughter,” he said.

Eventually, Floyd told the investigators what happened to Michael Hughes: He murdered the first-grader on the same day he kidnapped him.

They were driving from Oklahoma City to Dallas, and “Michael was being a typical 6-year-old. He was out of control, and that pushed Floyd over the edge,” Lobb said. “Floyd felt the pressure and he just ran out of patience.” Lobb vividly remembers the moment Floyd confessed. “He turned and looked at me and said, ‘I shot him twice in the back of the head to make it real quick.’”

Why did Floyd finally confess? “I think he just ran out of excuses,” Lobb said, adding that Floyd is now 72 and has serious health issues. With no date set for his execution, Lobb believes it is likely Floyd will die of natural causes on death row.

On the day of Michael’s murder, someone called the police and described a suspicious man with a young boy at an Oklahoma interstate rest area near the Texas border. That fit with Floyd’s story—he told Lobb he had buried the boy near the last interstate exit leaving Oklahoma.

With the help of the FBI’s Evidence Response Team and anthropologists from the University of Oklahoma, Lobb narrowed down a search area. After 20 years, nothing would likely remain of Michael’s body—even his bones would have been eaten by feral animals—but investigators thought they might find the two shell casings, or possibly metal eyelets from Michael’s sneakers. After two days of sifting dirt in a 2,000-square-foot area, though, no evidence was found.



**This childhood picture shows Suzanne Marie Sevakis near the time she was kidnapped by Franklin Delano Floyd. It took more than two decades for investigators to discover that the victim who died in a suspicious hit-and-run accident in Oklahoma City in 1990 was actually 20-year-old Sevakis.**

In the end, Floyd’s confession put to rest a 20-year-old murder case and revealed the true identity of Tonya Hughes, whose suspicious death remains unsolved. “That’s the one thing Floyd won’t talk about,” Lobb said.

The veteran investigator with more than two decades of experience hopes to interview Floyd again. Maybe more mysteries will be unraveled. “There is still a great deal we can learn from him,” Lobb said. “Maybe now that he is nearing the end of his life he will want to make a full accounting, to set the record straight about everything he has done.” For now, though, Lobb is content. “This has been one of the most fascinating cases I have ever worked.”

# Byte Out of History

## FBI Involvement in Early Election Fraud Case in Kansas City

Impartial and fair elections are the cornerstone of any democracy, and the FBI has a long history of investigating illegal activities that harm the elective process.

One of our earliest investigations involved Kansas City political fixer Tom Pendergast, who was threatened by the basic workings of democratic elections—in particular, by any election that didn't go his way. In the 1920s and 1930s, Pendergast, a former alderman, ran the political machine that controlled the electoral choices in Kansas City, Missouri, and he got rich in the process. Because of Pendergast's corrupt activities—including voter fraud and bribery—Kansas City became known as an open city where gangsters moved freely and prostitution, gambling, and drug enterprises flourished.

And, of course, election fraud flourished as well, along with its accompanying scare tactics. The 1934 primary election in Kansas City had been so violent that it became known as the “Bloody Election,” with thugs connected to the Pendergast machine committing acts of violence and intimidation against opponents and voters across the city. The fraudulent reporting of election results was even more damaging to the democratic process—precincts returned astronomical participation rates. Vote totals for machine candidates (Pendergast's picks) even exceeded the total population in several wards and precincts.

Tired of Pendergast's tight-fisted control of their city, a coalition of his opponents banded together for 1936 municipal elections and attempted to throw Pendergast's supporters out of office. But that

was not to be, at least not right away.

For the spring primary, fraud appeared to be the order of the day. U.S. Attorney Maurice Milligan of the Western District of Missouri later wrote that in one city ward, the vote ratio was 1,045 to 1, and in another, the ratio was 1,469 to 1—both in favor of the machine candidates. The sheer size of the margins suggested a serious problem.

In anticipation of the 1936 general election in the fall, Milligan called for a grand jury to convene and began to gather information. A federal judge from the district agreed, saying that there was “a crying need for the purification of the ballot in America” and authorizing Milligan to seize electoral records after the counts were submitted to investigate possible fraud. It would be the U.S. Marshals' job to gather and secure the evidence and the FBI's job to help analyze this voluminous material and collect additional evidence in the case.

On election morning, the Pendergast political machine was out in full force. Voting proceeded throughout the day and election officials tallied, recorded, reported, and sealed the records as they were supposed to. But at that point, the U.S. Marshals stepped in and claimed the records under grand jury warrant. By 8 p.m. that night, truckloads of ballots and other records—12 tons worth—were carted to the federal building in Kansas City and FBI agents began to examine them.

FBI Agent Charles Appel, the founder of the Bureau's Technical Laboratory, was point man, as his expertise was forensic document



**U.S. Attorney Maurice Milligan, Western District of Missouri, played a critical role in helping to uncover the crimes of Kansas City political fixer Tom Pendergast and his organization in the 1930s.**

examination. The first bag opened revealed that at least 95 ballots had been tampered with. Further analysis showed such fraud and other tinkering were systemic.

The first federal indictments for voter fraud were leveled in January 1937, and by the middle of 1938, 242 people had either pled guilty or been convicted at trial. Of those who chose to go to trial, they were convicted by juries of their peers—who perhaps were sending a message that corruption would no longer be tolerated in Kansas City.

Of course, Pendergast himself appeared unscathed at first, but his political machine was severely damaged. And these first cracks in his organization led to other challenges to his rule. Eventually, agents of the Internal Revenue Service were able to gather evidence against Pendergast on tax evasion charges related to a large kickback he had received, and the boss' rule was ended by a guilty plea and a stint in the Leavenworth federal penitentiary.



# Attacks on Arkansas Power Grid

## Perpetrator Sentenced to 15 Years

On August 21, 2013, the FBI's Little Rock Field Office was notified by a local energy provider about a downed 500,000-volt power line near an active railroad track in Cabot, Arkansas. A power outage ensued. Company officials and local law enforcement believed earlier that day, someone had climbed a 100-foot tall support tower and intentionally sawed off the shackles that held up the power line, which then fell across the railroad tracks. A short time later, a train struck the line and severed it.

The FBI was called into the matter because sabotaging an energy facility and causing more than \$100,000 in damage is a federal crime. According to energy company officials, the damage in this instance was \$550,000.

A search of the crime scene and subsequent investigative activity by FBI Little Rock's Joint Terrorism Task Force—aided by our local law enforcement partners and power company officials—revealed much about what had happened.

In addition to the power line's support tower shackles being cut with a hacksaw, someone had loosened most of the bolts holding the support tower to its cement base. Investigators believed that in a previous attempt to damage the support tower and take down the power line, the perpetrator had taken a steel cable—insulated in blue plastic hosing that's often used for pool maintenance—and tied one end to the bottom of the support tower and the other end to a tree across the railroad tracks in the hopes that a train would run into the cable, pulling down the entire support tower and possibly toppling several nearby towers. Instead, the cable simply snapped when hit by the train, and the

tower—and power line—remained in place. Pieces of the cable and the blue hosing from that attempt were found at the crime scene.

But then there were two more seemingly related incidents:

On September 29, 2013, an energy provider received an intruder alert at an extra-high voltage switching station in Scott, Arkansas, which was soon followed by a series of other alarms. Local law enforcement officers responded to find the station on fire. Damages in this instance exceeded \$4 million.

And on October 6, 2013, an energy provider near Jacksonville, Arkansas lost power for several hours, impacting thousands. Soon after, investigators found that a 115,000-volt transmission line had fallen after someone cut into two power poles and pulled one down using a tractor. Damages were close to \$50,000.

A few days later, on October 11, 2013, local law enforcement responded to reports of an explosion in a Jacksonville neighborhood and determined that it occurred under the power lines that ran alongside the residence of Jason Woodring, a self-employed pool maintenance worker who lived there with his mother. Because Woodring's residence was close to the location of the October 6 sabotage incident and because the tractor used to cut into the power poles in that incident was stolen from a location directly across the street from Woodring's home, local police suspected this particular explosion might be related to the previous acts of sabotage. They reached out to Bureau agents, who had noticed discarded blue hose at Woodring's house similar to that found at the August 21 incident.



**An electrical station fire in Arkansas was intentionally set by Jason Woodring. (Photo courtesy of Lonoke County Sheriff's Office.)**

During an interview with federal agents, Woodring confessed to all three incidents, as well as the explosion that brought law enforcement to his house (using a fishing pole, he had cast a piece of wire over the power lines near his home, which caused the blast). He later pled guilty.

While Woodring's motives for his activities were not clear, he did leave some vague anti-government messages at two of the crime scenes, and at his recent sentencing hearing, he told the judge that he was trying to help society. He also pled guilty to being an illegal drug user in possession of various firearms and ammunition.

Woodring was ordered by the judge to pay more than \$4 million in restitution to one energy company and nearly \$50,000 to another.

The power grid attacks, according to Eastern District of Arkansas U.S. Attorney Christopher Thyer, “had the potential to put many lives at risk. When we depend on electrical power not only for comfort and convenience but also for safety, security, and life-sustaining equipment, not knowing where the next attack would occur held the public hostage to an unknown attacker.”

But thanks to the collaboration between the FBI and its partners, that “unknown” attacker was identified and brought to justice.

# Loan Sharks Sentenced

## Albanian Crime Group Used Violence, Intimidation in Business Dealings

Loan sharking. It's a term that might conjure up historical images of shadowy organized crime figures handing out questionable loans at exorbitant interest rates to desperate customers, usually followed by threats of violence if the loans aren't paid off.

Unfortunately, loan sharks are alive and well in 2015 and continue to benefit from the financial misfortunes of others. Last month, the two top leaders of an Albanian criminal organization operating in the Philadelphia area were sentenced to lengthy federal prison terms for running a violent loan sharking and illegal gambling ring. Ylli Gjeli, the boss, and Fatimir Mustafaraj, the muscle, were convicted late last year after a six-week trial. Two other defendants were convicted at the same trial.

From 2002 to 2013, Gjeli and Mustafaraj led the multi-million-dollar criminal enterprise with two primary sources of income: loan sharking and illegal gambling. The illegal gambling arm of the operation included an online sports betting website that contributed more than \$2.9 million in gross profits to the group's criminal coffers. There was often crossover between the two arms of the organization—when customers couldn't cover their gambling losses, bookies would refer them to the loan sharking side of the house.

The illegal activity took place in Philadelphia bars and coffee houses owned or controlled by the organization. Besides the gambling operation, Gjeli, Mustafaraj, and company generated money by making loans to customers at interest rates that ranged from 104 percent to 395 percent and demanding weekly repayments.



**Members and associates of an Albanian criminal enterprise conducted much of their illegal activity in this Philadelphia bar they owned and in their pizza eatery next door.**

These repayment demands were almost always accompanied by acts of intimidation. Customers were menaced with firearms, hatchets, and threats of physical harm to themselves or family members. In a number of instances, perhaps to create the false impression that the Albanians were part of a larger and more powerful organization, customers were told that “people from New York” were willing to cause bodily harm to anyone who didn't pay up.

Gjeli and Mustafaraj not only directed the criminal activities of their underlings—who included debt collectors and bookies—they also got their own hands dirty by directly financing loans, intimidating and threatening violence against customers to collect loan payments, and physically assaulting subordinates and associates who stole from the organization or who didn't collect their debts on time.

According to Philadelphia FBI Special Agent in Charge Edward Hanko, Gjeli and Mustafaraj took advantage of their victims twice. “They provided loans at outrageous interest rates to those unable to obtain loans from traditional sources,” he explained, “and then used threats and violence to collect on those illegal loans.”

The investigation revealed that the Lion Bar, an establishment owned by Gjeli, served as the main hub of the organization's criminal

activities—it was where Gjeli, Mustafaraj, and their associates met with current and prospective borrowers. What they didn't realize was that one of their borrowers was actually an FBI undercover agent, and during one particular meeting, details of a \$50,000 loan were worked out with him. Gjeli informed our undercover agent that his limbs would be broken if he didn't pay back what he owed in a timely manner.

Also during the investigation, law enforcement was able to make more than 400 audio recordings and numerous surveillance videos of the criminal activity. By August 2013, arrests were made, including those of Gjeli and Mustafaraj. And the FBI executed a series of search warrants at related businesses, homes, vehicles, and a storage locker. Law enforcement recovered guns, cash, computers, phones, video surveillance, loan applications, loan ledgers, and gambling records. Fortunately, the group kept good records of its criminal activities, and much of the evidence seized in August was presented at trial.

That evidence, plus trial testimony from many of Gjeli's and Mustafaraj's customers—and even members of their own criminal organization—was enough to convince a jury of the defendants' guilt.

And as with many successful investigations, the FBI didn't do it alone: Our Philadelphia Field Office worked closely with the Pennsylvania State Police, New Jersey State Police, Montgomery County Detective Bureau, and the Internal Revenue Service to dismantle a very dangerous and prolific criminal enterprise.



# Former DuPont Employee Sentenced

## Involved in Foreign Conspiracy to Steal Trade Secrets

A second former DuPont employee—Edward Schulz—was recently sentenced for his role in a conspiracy led by a South Korean company to steal trade secrets related to Kevlar, a trademarked product developed and sold by DuPont.

Kevlar, an incredibly strong synthetic fiber developed by the U.S.-based DuPont 50 years ago, is used around the world in body armor, fiber optic cables, automotive and industrial products, and a variety of other applications. Soon after its development, DuPont trademarked Kevlar, mass-produced it, and put it on the market. But none of this was easy—the company had expended untold resources on Kevlar’s research and development, ground-breaking manufacturing processes, and innovative business plans (collectively known as “trade secrets”) before the product became a success.

DuPont’s hard work and ingenuity paid off. But there are companies who believe that their road to success can be paved with someone else’s hard work and ingenuity. That was the case with executives from a South Korean company called Kolon Industries who, interested in developing their own Kevlar-like product to compete with DuPont, put a plan in motion to steal proprietary information related to Kevlar—primarily by going after former DuPont employees who might be in a position to have such information.

Stealing another company’s trade secrets is a federal crime, and, after an FBI investigation by our field office in Richmond (where DuPont has a large plant)—with the assistance of the Department of Commerce’s Export Enforcement

Office—Kolon Industries and five of its executives were indicted on theft of trade secrets charges. The company pled guilty to the charges in April of this year and was ordered to pay \$85 million in criminal fines and \$275 million in restitution.

Edward Schulz—who worked for DuPont for just over 30 years before he left around 2000—was responsible for technical research and development relating to Kevlar. Despite a signed agreement barring him from disclosing DuPont’s secret or confidential information during or after employment, he held on to numerous DuPont documents when he left the company. So when Kolon came calling and Schulz accepted their offer of a consulting job, they soon began questioning him about Kevlar, and he willingly turned over some of the proprietary information he had in his possession.

Another long-time former DuPont employee—engineer and salesman Michael David Mitchell—was also caught up in the conspiracy and was charged with and pled guilty to theft of trade secrets several years ago. Mitchell, fired by DuPont for performance reasons in 2007, had signed the same non-disclosure agreement as Schulz, but he also held on to some proprietary information when he left. While looking for another job, he met with Kolon representatives and eventually was hired by them as a consultant.

Mitchell shared with Kolon some of the proprietary information he had, but when Kolon representatives began asking him extremely technical questions on Kevlar, he reached out to former and current DuPont employees for answers. Word of his activities, however, got



Shown above are some of the DuPont-related items seized by the FBI during a search of former DuPont employee Michael David Mitchell’s residence.

back to DuPont management, who reached out to the FBI with their concerns.

Eventually, Mitchell agreed to cooperate with law enforcement and made numerous recorded phone calls and exchanged e-mails with Kolon representatives. He also hosted a face-to-face meeting with representatives in a Richmond hotel, which was audiotaped and videotaped by the Bureau.

This case would have been nearly impossible to make without the assistance of DuPont. In addition to the company coming to us initially about the attempts to steal their trade secrets, DuPont worked with us to understand and organize more than a million pages of Kevlar-related documents and hundreds of hours of audio recordings, which enabled the case to move forward quickly. And the FBI and the Department of Justice worked to ensure that DuPont’s proprietary information—much of which was used as evidence—wasn’t disclosed publicly.

As a result of its experience, DuPont enhanced efforts to protect its proprietary information. Other American companies, if they haven’t already done so, need to follow suit—the desire to steal U.S. business trade secrets continues unabated.

# Medicare Fraud

## Hospice Owner Falsified Numerous Claims

The overwhelming majority of people who go into the health care industry do it because they want to help people. Unfortunately, there are also some unscrupulous individuals who do it because they think they can take advantage of the health care system for their own financial gain.

That's just what happened in the case of an Oklahoma hospice executive. Paula Kluding, owner of Prairie View Hospice, Inc., located in Chandler, Oklahoma, submitted millions of dollars' worth of fraudulent claims to the federal Medicare program. But after a thorough investigation by the FBI and our partners at the U.S. Department of Health and Human Services' Office of Inspector General, Kluding was convicted of Medicare fraud and other related charges at trial and was recently sentenced to a federal prison term. She was also ordered to pay \$2.5 million in restitution to Medicare.

Hospice care, by definition, consists of health care, medication, certain medical equipment, and other goods and services provided to terminally ill patients. Prairie View Hospice was ostensibly in the business of doing just that and advertised its services for patients in nursing care facilities and at home. And as a Medicare-approved provider of hospice care, Prairie View agreed that it would comply with all Medicare-related laws and regulations, including those that required submissions of truthful and accurate claims for reimbursement.

But from July 2010 until July 2013, Kluding did not comply with those laws and regulations in her dealings with Medicare. In fact, she conspired—with her general manager and two nurses—to



Shown is the Chandler, Oklahoma office of Prairie View Hospice, Inc., whose owner—Patricia Kluding—was convicted of running a Medicare fraud scheme.

actually conceal the true medical conditions of hospice patients and the true quality and quantity of their care in order to continue receiving payments from Medicare. (The general manager and both nurses were later charged in the scheme and ultimately pled guilty.)

How did Kluding conceal the true medical conditions of her patients? For one, she directed certain medical documents be changed or written a certain way to make it appear as if nurses had visited patients or conducted assessments at the regular intervals required by Medicare—when, in fact, they hadn't. She also directed that nursing notes be falsified to make it appear that patients were in worse health than they actually were.

Typically, hospice care is offered for those with a life expectancy of six months or less. Our investigation revealed that many Prairie View Hospice patients received care for five, six, even seven years.

Making Kluding's criminal activity seem even riskier was the fact that at the time, Prairie View Hospice was part of a broader Medicare audit being conducted

in the state. And to make matters worse, she gave falsified documents to the Medicare subcontractor performing the audit when asked to provide records of patient files and Medicare claims.

A pivotal point in the investigation came during the first interview with one of the two nurses charged in the case—she made a full confession and helped provide the necessary probable cause to obtain search warrants.

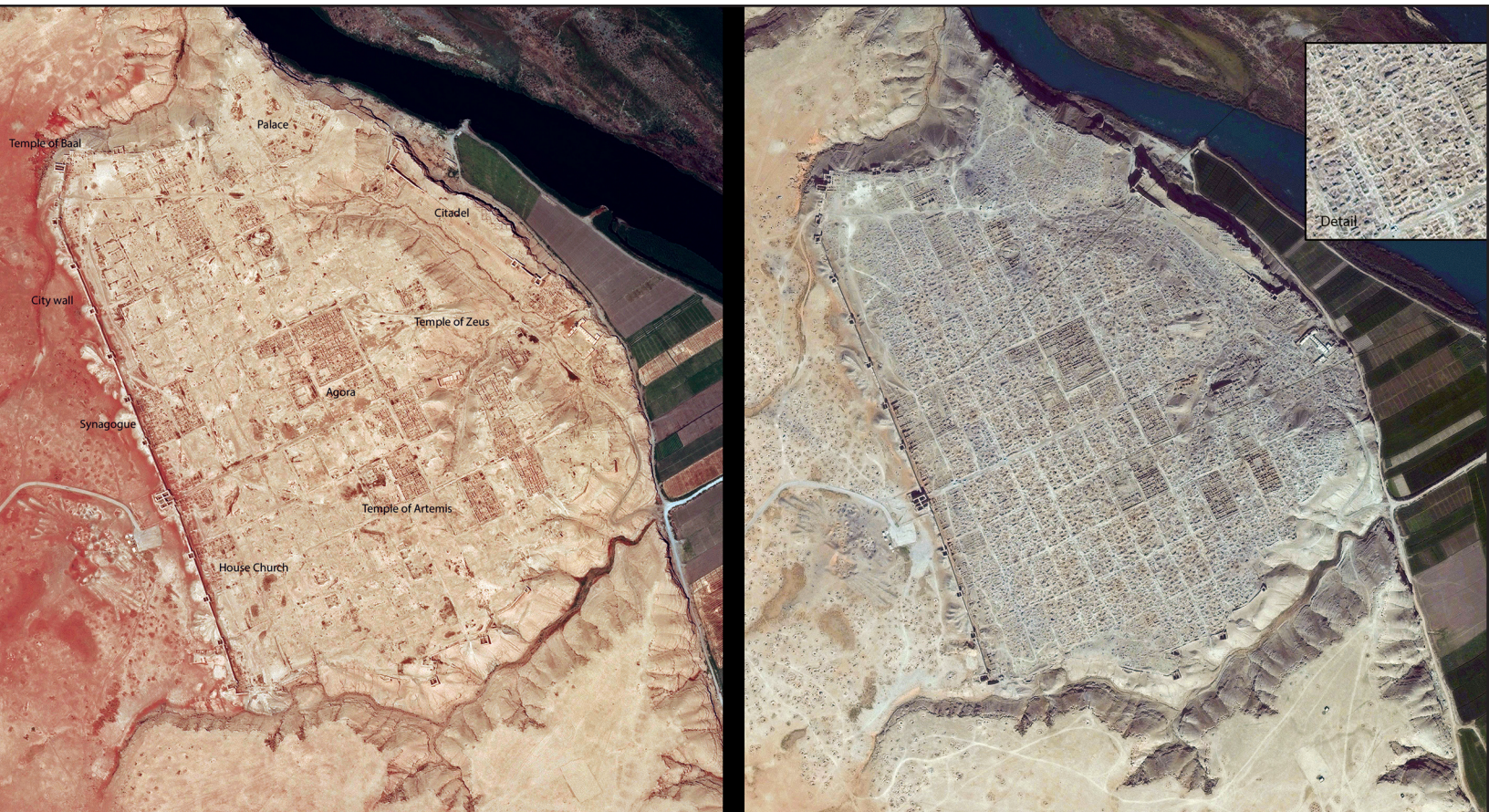
Kluding had pocketed a substantial portion of the Medicare payments she received, using Prairie View Hospice's account as well as two other medical business accounts as her personal checkbook. A review of her banking records showed that she moved money between her business accounts and personal account whenever she needed additional money to fund her lavish lifestyle—which included a 6,000-square-foot home on hundreds of acres of land.

But that lavish lifestyle is over: In addition to the \$2.5 million in restitution, Kluding owes an additional \$5.4 million to Medicare for overpayments.



# ISIL and Antiquities Trafficking

## FBI Warns Dealers, Collectors About Terrorist Loot



Satellite imagery of Dura Europos, a 150-acre site in Syria dating to 300 B.C., shows how it looked in 2012 (left) and as it appeared in 2014 covered by looters' pits.

The FBI is alerting art collectors and dealers to be particularly careful trading Near Eastern antiquities, warning that artifacts plundered by terrorist organizations such as ISIL are entering the marketplace.

"We now have credible reports that U.S. persons have been offered cultural property that appears to have been removed from Syria and Iraq recently," said Bonnie Magness-Gardiner, manager of the FBI's Art Theft Program.

The Bureau is asking U.S. art and antiquities market leaders to spread the word that preventing illegally obtained artifacts from reaching the market helps stem the transfer of funds to terrorists.

In a single-page document titled

*ISIL Antiquities Trafficking*, the FBI asks leaders in the field to disseminate the following message:

- Please be cautious when purchasing items from this region. Keep in mind that antiquities from Iraq remain subject to Office of Foreign Assets Control sanctions under the Iraq Stabilization and Insurgency Sanctions Regulations (31 CFR part 576).
- Purchasing an object looted and/or sold by the Islamic State may provide financial support to a terrorist organization and could be prosecuted under 18 USC 233A.
- Robust due diligence is necessary when purchasing any Syrian or Iraqi antiquities or other cultural

property in the U.S. or when purchasing elsewhere using U.S. funds.

In February, the United Nations Security Council unanimously passed Resolution 2199, which obligates member states to take steps to prevent terrorist groups in Iraq and Syria from receiving donations and from benefiting from trade in oil, antiquities, and hostages.

As part of a broad U.S. government response, the Department of State this spring published satellite imagery showing industrial-level looting at Syrian and Iraqi archaeological sites. In a May raid against the now deceased ISIL finance chief Abu Sayyaf in Syria, U.S. Special Operations Forces



recovered a significant cache of archaeological and historical objects and fragments. According to the State Department's Bureau of Educational and Cultural Affairs, "The cache represents significant primary evidence of looting at archaeological sites in Syria and Iraq, theft from regional museums, and the stockpiling of these spoils for likely sale on the international market."


The looted materials, which were returned to the Iraq National Museum, included coins, pottery, glass, ivory, stone, jewelry, figurines, bowls, and manuscripts. Types of objects subject to looting appear in the International Council of Museums' (ICOM) Red Lists of antiquities at risk posted on the

State Department website. Here, collectors and dealers can view and learn to recognize the kinds of objects that have been looted from cultural sites, stolen from museums and churches, and illicitly trafficked. Syria and Iraq each have emergency Red Lists.

The significance of valuable cultural antiquities as currency to ISIL was brought into sharp relief earlier this month in Palmyra, Syria—a UNESCO World Heritage site dating to the second millennium B.C.—with the public execution of a Syrian art scholar who reportedly refused to reveal to ISIL the location of valuable antiquities.

In the U.S., meanwhile, buyers may want to consult the Red Lists and should pay special attention to an object's origin. Buyers should ask many questions such as: *Where did this come from? When did it come into the country? Does it have an export license from the country of origin?*


"Check and verify provenance, importation, and other documents," said Magness-Gardiner. "You have to be very careful when you're buying. We don't want to say don't buy anything at all. There's a lot of legitimate material circulating in the marketplace. What we're trying to say is, don't allow these pieces that could potentially support terrorism to be part of the trade."



## ISIL Antiquities Trafficking









Photos of antiquities courtesy of U.S. Department of State.









Satellite images have shown industrial-level looting at Syrian and Iraqi archaeological sites. The FBI has received reports from credible sources who have been approached by individuals trying to sell objects that appear to have been illegally looted and trafficked from Syria or Iraq, likely by those associated with the Islamic State in Iraq and the Levant (ISIL) terrorist group.

Recognizing art and antiquities trafficking as a terrorist financing tool, in February 2015, the United Nations Security Council unanimously voted for Resolution 2199, which obligates member states (including the U.S.) to take steps to prevent terrorist groups in Iraq and Syria from receiving donations and from benefiting from trade in oil, antiquities, and hostages.

Recognizing that the legitimate market for art and antiquities is a component of the U.S. economy, the FBI is asking for help in preventing illicitly obtained art and antiquities from reaching the market and in preventing any transfer of funds from benefiting ISIL.

The FBI is requesting help from art and antiquities market leaders in halting trade in looted and stolen artifacts from Syria and Iraq by asking them to disseminate the following message to their members, clients, and constituents:

- Please be cautious when purchasing items from this region. Keep in mind that antiquities from Iraq remain subject to Office of Foreign Assets Control sanctions under the Iraq Stabilization and Insurgency Sanctions Regulations (31 CFR part 576).
- Purchasing an object looted and/or sold by the Islamic State may provide financial support to a terrorist organization and could be prosecuted under 18 USC 2339A.
- Robust due diligence is necessary when purchasing any Syrian or Iraqi antiquities or other cultural property in the U.S. or when purchasing elsewhere using U.S. funds.

Individuals and institutions in the trade, professional, and academic communities have been instrumental in the success of many FBI cultural property investigations and their continued input and cooperation is needed to prevent ISIL-generated income from looted objects.

The FBI is devoted to combating crime and threats to national security and wants to help keep the market clean for legitimate business.

Please report any suspect solicitations to the FBI:

- tips.fbi.gov
- Local FBI field office
- 1-800-CALL-FBI

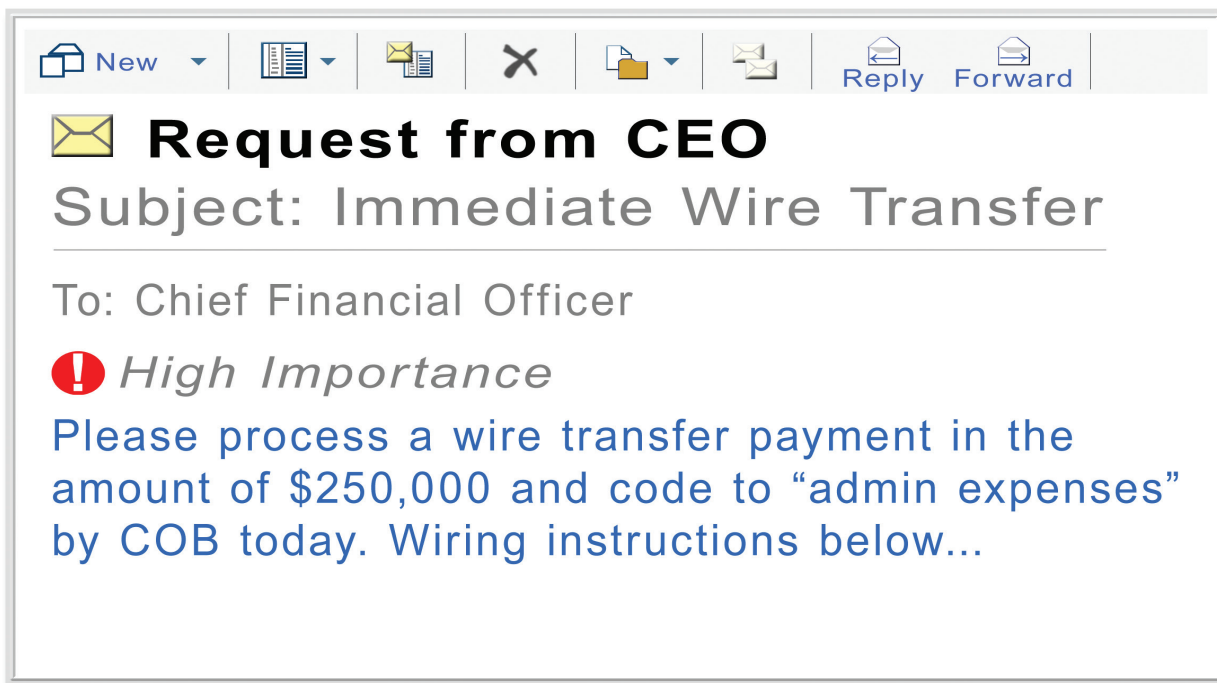
August 25, 2015

The FBI released a flyer requesting help from art and antiquities market leaders in halting trade in looted and stolen artifacts from Syria and Iraq.



# Business E-Mail Compromise

## An Emerging Global Threat



The accountant for a U.S. company recently received an e-mail from her chief executive, who was on vacation out of the country, requesting a transfer of funds on a time-sensitive acquisition that required completion by the end of the day. The CEO said a lawyer would contact the accountant to provide further details.

“It was not unusual for me to receive e-mails requesting a transfer of funds,” the accountant later wrote, and when she was contacted by the lawyer via e-mail, she noted the appropriate letter of authorization—including her CEO’s signature over the company’s seal—and followed the instructions to wire more than \$737,000 to a bank in China.

The next day, when the CEO happened to call regarding another matter, the accountant mentioned that she had completed the wire transfer the day before. The CEO said he had never sent the e-mail and knew nothing about the alleged acquisition.

The company was the victim of a business e-mail compromise (BEC), a growing financial fraud that is more sophisticated than any similar scam the FBI has seen before and one—in its various forms—that has resulted in actual and attempted losses of more than a billion dollars to businesses worldwide.

### *“The FBI takes the BEC threat very seriously.”*

“BEC is a serious threat on a global scale,” said FBI Special Agent Maxwell Marker, who oversees the Bureau’s Transnational Organized Crime–Eastern Hemisphere Section in the Criminal Investigative Division. “It’s a prime example of organized crime groups engaging in large-scale, computer-enabled fraud, and the losses are staggering.”

Since the FBI’s Internet Crime Complaint Center (IC3) began tracking BEC scams in late 2013, it has compiled statistics on more than 7,000 U.S. companies that

have been victimized—with total dollar losses exceeding \$740 million. That doesn’t include victims outside the U.S. and unreported losses.

The scammers, believed to be members of organized crime groups from Africa, Eastern Europe, and the Middle East, primarily target businesses that work with foreign suppliers or regularly perform wire transfer payments. The scam succeeds by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques. Businesses of all sizes are targeted, and the fraud is proliferating.

According to IC3, since the beginning of 2015 there has been a 270 percent increase in identified BEC victims. Victim companies have come from all 50 U.S. states and nearly 80 countries abroad. The majority of the fraudulent transfers end up in Chinese banks.

Not long ago, e-mail scams were fairly easy to spot. The Nigerian

lottery and other fraud attempts that arrived in personal and business e-mail inboxes were transparent in their amateurism. Now, the scammers' methods are extremely sophisticated.

"They know how to perpetuate the scam without raising suspicions," Marker said. "They have excellent tradecraft, and they do their homework. They use language specific to the company they are targeting, along with dollar amounts that lend legitimacy to the fraud. The days of these e-mails having horrible grammar and being easily identified are largely behind us."

To make matters worse, the criminals often employ malware to infiltrate company networks, gaining access to legitimate e-mail threads about billing and invoices they can use to ensure the suspicions of an accountant or financial officer aren't raised when a fraudulent wire transfer is requested.

Instead of making a payment to a trusted supplier, the scammers direct payment to their own accounts. Sometimes they succeed at this by switching a trusted bank account number by a single digit. "The criminals have become experts at imitating invoices and accounts," Marker said. "And when a wire transfer happens," he added, "the window of time to identify the fraud and recover the funds before they are moved out of reach is extremely short."

In the case mentioned above—reported to the IC3 in June—after the accountant spoke to her CEO on the phone, she immediately reviewed the e-mail thread. "I noticed the first e-mail I received from the CEO was missing one

letter; instead of .com, it read .co." On closer inspection, the attachment provided by the "lawyer" revealed that the CEO's signature was forged and the company seal appeared to be cut and pasted from the company's public website. Further assisting the perpetrators, the website also listed the company's executive officers and their e-mail addresses and identified specific global media events the CEO would attend during the calendar year.

The FBI's Criminal, Cyber, and International Operations Divisions are coordinating efforts to identify and dismantle BEC criminal groups. "We are applying all our investigative techniques to the threat," Marker said, "including forensic accounting, human source and undercover operations, and cyber aspects such as tracking IP addresses and analyzing the malware used to carry out network intrusions. We are working with our foreign partners as well, who are seeing the same issues." He stressed that companies should make themselves aware of the BEC threat and take measures to avoid becoming victims (see sidebar).

If your company has been victimized by a BEC scam, it is important to act quickly. Contact your financial institution immediately and request that they contact the financial institution where the fraudulent transfer was sent. Next, call the FBI, and also file a complaint—regardless of dollar loss—with the IC3.

"The FBI takes the BEC threat very seriously," Marker said, "and we are working with our law enforcement partners around the world to identify these criminals and bring them to justice."

### How to Avoid Becoming a Victim of a BEC Scam

In October 2013, the Internet Crime Complaint Center (IC3) began receiving complaints from businesses about trusted suppliers requesting wire transfers that ended up in banks overseas—and turned out to be bogus requests. Since then, losses from the business e-mail compromise (BEC) scam have been significant.

"For victims reporting a monetary loss to the IC3, the average individual loss is about \$6,000," said Ellen Oliveto, an FBI analyst assigned to the center. "The average loss to BEC victims is \$130,000." IC3 offers the following tips to businesses to avoid being victimized by the scam (a more detailed list of strategies is available at [www.ic3.gov](http://www.ic3.gov)):

- Verify changes in vendor payment location and confirm requests for transfer of funds.
- Be wary of free, web-based e-mail accounts, which are more susceptible to being hacked.
- Be careful when posting financial and personnel information to social media and company websites.
- Regarding wire transfer payments, be suspicious of requests for secrecy or pressure to take action quickly.
- Consider financial security procedures that include a two-step verification process for wire transfer payments.
- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail but not exactly the same. For example, .co instead of .com.
- If possible, register all Internet domains that are slightly different than the actual company domain.
- Know the habits of your customers, including the reason, detail, and amount of payments. Beware of any significant changes.



# Jewelry Store Robberies

Dallas Task Force Helps Put Violent Criminals Behind Bars



This stolen jewelry from several armed robberies—much of it with price tags still on—was found in the Texas residence of Mark D. Whitfield, who, along with Michael Demon Jackson, was later convicted of the crimes.



Two Texas men who committed violent jewelry store robberies in the Dallas/Fort Worth area were recently sentenced to lengthy prison terms thanks to an FBI-led task force that helped bring them to justice. The case is a classic example of local and federal law enforcement officers working together to make their communities safer.

For a seven-month period between 2013 and 2014, Michael Demon Jackson and Mark D. Whitfield robbed numerous jewelry stores at gunpoint, in part to feed their heroin habits. Last May, after pleading guilty to the crimes, Jackson was sentenced to 594 months in federal prison, just shy of 50 years. In June, Whitfield received a 309-month prison term.

***“Being able to bring federal charges in violent criminal cases is one of the strengths of the task force.”***

“Jackson had a previous murder conviction, and the judge took that into consideration,” said FBI Special Agent Gil Balli, who supervises the Dallas Violent Crimes Task Force that investigated the case. The fact that both men were charged federally resulted in stiffer sentences and no chance of parole.

“Being able to bring federal charges in violent criminal cases is one of the strengths of the task force,” Balli said. Established two years ago, the task force consists of FBI agents and officers from the Dallas Police Department and other local police departments from Garland and Carrollton, Texas. When necessary, the task force partners

with other state and federal agencies.

“Our mission,” Balli said, “is to target criminal groups and individuals, including fugitives, who commit the worst violent crimes in our area.”

***“It was very traumatic for the victims.”***

Balli receives daily updates about robberies that have occurred in the Dallas/Fort Worth area in the previous 24 hours. He consults with Dallas Police Department officials and other task force members about which crimes might rise to the level of task force involvement. “We all exchange intelligence on a daily basis,” he said, adding, “We are looking at the most violent offenders in our communities, who often commit serial robberies.”

Jackson and Whitfield fit that description. The pair targeted jewelry stores in shopping malls without good security and where female sales clerks worked alone. Whitfield would enter the store pretending to be a customer interested in making a purchase. When the clerk opened the display case, Jackson came in brandishing a gun.

“He would push the clerks to the ground, put the gun to the back of their heads, and threaten to kill them,” said Noe Camacho, a Dallas Police Department detective on the task force. “It was very traumatic for the victims.”

After several robberies, investigators had surveillance video from inside the stores, and not much else. But during an April 2014 robbery in Lewisville, Texas, a person saw two men running out of the mall and took

a picture of the car they drove away in—a red Mitsubishi Galant. The license plate was not visible, but investigators noticed that the passenger-side mirror was missing.

Camacho spent the next five days going through every traffic ticket issued in the area involving Mitsubishi Galants. Cross-referencing any tickets to drivers with criminal records, he found that Whitfield had recently been stopped by an officer who noted in his report that there was another man in the car and that they had a number of new watches in the vehicle.

“Whitfield’s criminal record had a long history of jewelry theft,” Camacho said. “We knew we were on the right track.” Task force members conducted surveillance and saw that Whitfield’s car was missing a passenger-side mirror.

***“It was very satisfying to get these guys off the street. They were dangerous individuals, and now they are no longer a threat to the community.”***

A search warrant was obtained, and when Whitfield’s house was searched and the pair was arrested, stolen jewelry from the robberies—much of it with price tags still on—was found in the residence.

“It was very satisfying to get these guys off the street,” Camacho said. “They were dangerous individuals, and now they are no longer a threat to the community.”



# Steroids Dealer Sentenced

## Advertised Products Online

Anabolic steroids, according to the National Institute on Drug Abuse, are the common name for synthetic variants of the male sex hormone testosterone. While these drugs are legally prescribed to treat certain medical conditions, they are also abused by some athletes, body builders, and others in attempts to enhance performance.

Because of their potential for abuse and the possibility of them causing serious health problems if misused, anabolic steroids have also been classified as a Schedule III drug under the federal Controlled Substances Act, which regulates the manufacture, possession, distribution, and use of certain substances. Recently, after a joint FBI/U.S. Postal Inspection Service (USPIS) investigation, a 43-year-old Virginia man, who had no license to distribute anabolic steroids and no prescription for the drug, pled guilty in federal court to his role in a steroid distribution conspiracy. This past July, that individual—Carl Macchiarulo—was sentenced to serve four years in prison.

During the investigation, FBI and USPIS investigators were assisted by the Drug Enforcement Administration and U.S. Customs and Border Protection (CBP).

Between December 2012 and September 2014, Macchiarulo owned and operated an illegal anabolic steroid business known as CK Labs out of the Midlothian home he shared with his wife and children. The lab was located in a room that only he had access to.

Not licensed to run a lab, Macchiarulo was also not a medical professional nor a chemistry expert. But despite all that, he purchased—from suppliers in China, Europe, and elsewhere—



One of the ampules of anabolic steroids seized by law enforcement during a search of Carl Macchiarulo's home in Midlothian, Virginia.

various raw anabolic steroid powders and pills to manufacture them into finished products and sell them.

Using phony names, Macchiarulo usually e-mailed his orders to his overseas suppliers and sent payments through money transfer services, keeping individual payments low so he wouldn't have to show identification. And he had his purchases sent either to his residence or to post office boxes opened under fictitious business names.

To avoid detection by CBP officials, suppliers usually sent their products to Macchiarulo in decoy packaging—looking like food or beverage products, toys, etc.

Once Macchiarulo received the steroids, he manufactured the raw products into a finished product for distribution under the CK Labs name. He even had his own logo—a bulldog. To market his merchandise, he bought ads and promoted his fake company—and its very real product—on websites known for advertising anabolic steroids.

Customers from more than 30 states contacted Macchiarulo by e-mail to place orders; they followed up by mailing him cash or prepaid money cards. He then packaged his products and, using a fictitious name and return address, took his parcels to the local U.S. post office.

But his plan was not as foolproof as he thought: As a result of investigative tips, USPIS and CPB eventually seized several of Macchiarulo's incoming and outgoing packages and, through testing, identified their primary contents as anabolic steroids.

Investigators from the FBI Richmond Field Office and the USPIS, after conducting surveillances of Macchiarulo and undertaking other investigative measures, had enough to obtain a search warrant for his home in September 2014.

Once inside, they found a treasure trove of evidence—thousands of tablets, pills, and liquid ampules containing anabolic steroids; equipment used in the manufacture of finished anabolic steroid products; printed copies of e-mails containing order and payment information from Macchiarulo's customers; envelopes and packages used to send the steroids; and more than \$100,000 in cash, some from the proceeds of the business.

Macchiarulo later surrendered to the government an additional \$57,000 in criminal proceeds.

As a result of this multi-agency effort, law enforcement successfully shut down an operation that made a potentially dangerous substance available—without restriction—to anyone willing to pay for it.



# La Cosa Nostra

## Lengthy Prison Terms for Lucchese Crime Family Members

In a world inhabited by international cyber criminals and violent terrorists, it would be easy to think of La Cosa Nostra—the Mafia—as a throwback to a bygone era. But a recent New Jersey case involving the Lucchese crime family is proof that traditional organized crime can still be a potent threat.

Members and associates of the Lucchese organized crime family—one of the families traditionally associated with La Cosa Nostra (LCN)—were recently sentenced to lengthy prison terms in New Jersey for a financial fraud scheme that illegally netted millions of dollars.

Nicodemo “Nicky” Scarfo, Jr., whose imprisoned father was an LCN crime boss in Philadelphia, was sentenced in July to 30 years in prison for racketeering, securities and wire fraud, and other charges related to the 2007 illegal takeover of FirstPlus Financial Group Inc. (FPFG), a publicly held company in Texas. His associate, Salvatore Pelullo, also received a 30-year term. Brothers William and John Maxwell received 20- and 10-year terms, respectively.

“Essentially, Scarfo and Pelullo used extortion and other illegal means to gain control of the company,” said Special Agent Joe Gilson, who investigated the case from the FBI’s Atlantic City Resident Agency in New Jersey. “And then they systematically looted the company.”

FPFG, once a billion-dollar financial organization that specialized in mortgages, had filed for bankruptcy. The company was dormant, said Special Agent Bill Hyland, who assisted in the investigation, “but still had assets,



Nicodemo “Nicky” Scarfo, Jr. and his La Cosa Nostra associate Salvatore Pelullo used some of the millions they illegally siphoned from FirstPlus Financial Group Inc. to buy this airplane.

thanks to the continued proceeds from all the mortgages it had financed.”

In 2007, Pelullo and Scarfo used threats and other tactics to intimidate and remove FPFG’s management and board of directors. They were replaced with Mafia associates, including the Maxwell brothers—William was named special counsel to FPFG, while John became the company’s CEO.

“Within several weeks of gaining control,” Gilson said, “Pelullo and Scarfo had lined their pockets with \$7 million. Before they were arrested in 2011, more than \$12 million was illegally funneled to them—money that rightfully belonged to the company’s stockholders.

The investigation revealed that between 2007 and 2008, Scarfo received \$33,000 per month from FPFG as a “consultant”—at a time when he was on home detention in New Jersey for violating his parole from a previous conviction. The money was being paid to a shell company controlled by Scarfo. Pelullo, using a different shell company, had a similar deal. With their ill-gotten gains, the mobsters purchased an airplane, a yacht, and expensive jewelry.

“Complicated financial crimes are not normally the strong suit of LCN,” Gilson noted. But Pelullo, who had two previous federal fraud convictions, “was a persuasive con man. He could maintain an air of legitimacy, but behind the scenes everything was a fraud.”

Using a variety of investigative techniques, including a court-ordered wiretap (monitored by retired FBI agents, some of whom had helped put Scarfo’s father behind bars), investigators unraveled the scam with the help of federal partners including the Department of Labor and the Bureau of Alcohol, Tobacco, Firearms, and Explosives. During the more than five-year investigation, a million pages of paper documents were analyzed and the contents of more than 100 computers were searched.

Scarfo, Pelullo, the Maxwells, and others associated with the fraud were convicted in 2014. “We feel great that our team was able to put a stop to these crimes and bring the subjects to justice,” Gilson said. “The FBI remains vigilant against all types of organized crime, including LCN.”



# Community Outreach

## Director Comey Praises Citizens Academy Alumni Association

Alumni Association President Tammy Denbo describes the essential mission of the organization and the role of FBI Citizens Academies.



Citizens Academy class members receive hands-on training from agents and experts from the FBI Laboratory and Training Divisions.

The Citizens Academy—one of the FBI's most successful community outreach programs—is designed to give civic, business, and religious leaders around the country a firsthand look at how the Bureau investigates crimes and deals with national security threats.

More than 18,000 people have graduated from the program, and many then join one of the 60 non-profit alumni associations nationwide whose mission is to support the FBI through volunteer community action. Last week in San Francisco, at the alumni group's annual leadership conference, Director James Comey commended participants for their efforts.

"You are part of a community that includes all of us inside the FBI and a lot of people who are doing community service outside the FBI," Comey said, describing alumni association members as indispensable to the Bureau.

"Everything the FBI tries to accomplish depends upon the American people believing us, trusting us, and seeing us for what I believe we are—honest, competent, and independent," he explained. "The problem we face is that most people don't get a clear look at us. Most people see us only as what they see on TV and in the movies."

Through the Bureau's community outreach efforts, Comey said, "We

work hard to get people to try and know us, and there is nothing as important in that effort as the Citizens Academy. We invite in leaders from all walks of life, and we say, 'Take a look at us, form your own conclusions, and then participate in conversations about us with the American people.'"

Tammy Denbo is a case in point. Despite being a former assistant state attorney near Tampa Bay, Florida, Denbo said, "I had no idea about the inner workings of the FBI and how the organization works to keep the country safe. I found the Citizens Academy to be an incredibly rewarding experience."





FBI Director James Comey addresses members of the National Citizens Academy Alumni Association at the group's annual leadership conference in San Francisco on September 3, 2015.



Participants receive instruction on shooting firearms, taking fingerprints, collecting evidence, and more.

After she graduated from the program, Denbo joined her local alumni association chapter and eventually became its president. At last week's conference, she was installed as the National Citizens Academy Alumni Association president.

"I wanted to find a way to give back to the FBI for everything they have given to me," she said, noting that alumni association members reflect the country's diverse communities and represent a direct conduit between those communities and the FBI.

From a national perspective, the alumni association undertakes initiatives such as distributing child

safety information and educating the public about human trafficking. In addition, individual chapters are free to pursue their own projects, depending on the needs of the community.

"We also try to inform people that the FBI is not just coming to knock on the door and make arrests," she said. "We help people understand that the FBI is actively engaged in trying to prevent crime and making neighborhoods safer." She added that each of the 60 Citizens Academy Alumni Association chapters are distinct entities from the FBI and receive no taxpayer dollars. Operating funds are raised through sponsorships and dues.

"What you are engaged in is public service," Comey told the group in San Francisco, "and your commitment is incredibly important to the FBI." He added, "I just flew all the way across the country for no other reason than to thank you. You are making a tremendous difference for the Bureau and for the entire nation."



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/caaacconference](http://www.fbi.gov/caaacconference).



# Man Sentenced for Orchestrating ‘Cramming’ Scheme

Unauthorized Charges Placed on Victims’ Phone Bills



It’s a problem that has bedeviled landline telephone users for a while now, but is increasingly causing headaches for mobile phone users as well. It’s called cramming, and it involves a third party placing unauthorized charges on your wired, wireless, or bundled services telephone bill. The Federal Communications Commission (FCC) estimates that cramming has impacted tens of millions of American households.

Cramming practitioners take advantage of what’s known as

local exchange carrier (LEC) billing, which allows users of particular electronic products or services—like ringtones, cell phone wallpaper, premium text messages of sports scores or daily horoscopes, etc.—to be billed through their local telephone company accounts rather than directly from the providers of the product or service. LEC billing is lawful, as long as the customer is aware of and has agreed to these charges. But when extra charges are placed on customers’ bills without their knowledge or consent, it’s cramming.

The FCC and the Federal Trade Commission (FTC) routinely undertake civil enforcement actions to punish those responsible for cramming and to provide financial relief for the victims. But occasionally, a cramming scheme is so egregious—in terms number of victims, how much money is lost, and how widespread it is—that the FBI pursues a criminal fraud case against the accused. That’s what happened in the joint FBI/Internal Revenue (IRS) investigation of a Montana man—Steven Vincent Sann—who was recently sentenced

to a federal prison term for orchestrating a nationwide scheme involving approximately \$70 million in unauthorized fees being charged to phone bills associated with more than one million landline phone numbers.

Sann first came to the attention of the FBI during the course of a drug investigation. An analysis of his bank accounts revealed that he was receiving large amounts of money from billing aggregators known for working with phone companies to facilitate the placing of charges on phone bills by third parties. Investigators, following the money trail, found that Sann was using LEC billing to charge for a standalone voicemail and fax service he was marketing through several companies he managed.

After looking through Sann's business records, investigators determined that he was actually running a cramming operation. His companies had received numerous cramming complaints, but Sann didn't report them to the billing aggregators, as he was contractually obligated to do, because that would have jeopardized his scheme. Additional details and evidence of the cramming operation came out in interviews with victims, billing aggregators, phone companies, Sann's employees, and others.

Citing the size and complexity of the case, the FBI agent who worked the investigation acknowledged the contributions of his counterpart at the IRS. "We worked together every step of the way—formulating strategy, conducting interviews, and analyzing financial records," he explained.

How did the scheme work? Sann contracted with various billing

aggregators and provided them with the consumer telephone numbers to be billed. The aggregators, in turn, provided the information to the phone companies, which placed the charges for Sann's product on the bills associated with each telephone number. When the customers paid their bills, the phone companies—after taking out their fees—forwarded the remainder of the money to the billing aggregators, who took out their fees. The remaining funds were deposited into Sann's accounts.

*Crammers rely on a number of tricks to confuse consumers into paying for services they didn't authorize.*

The primary ingredient in any cramming scheme is a working phone number. Investigators believed that Sann could have obtained his numbers from lists he bought from marketers and/or from victims entering their phone numbers on misleading website advertisements.

Crammers like Sann rely on a number of tricks to confuse consumers into paying for services they didn't authorize or that cost more than they were led to believe. For instance, unauthorized charges are usually given general and innocuous-sounding names, like service fee, service charge, voicemail, mail server, and calling plan. And the charges, usually monthly, are often relatively small, anywhere from \$9.95 to \$24.95.

Consumer awareness is the key to minimizing the financial damages caused by crammers (see sidebar). And if you think you've been the

victim of cramming, contact your telephone service provider and file a complaint online with the FCC or the FTC.

**Tips to Protect Yourself Against Cramming**

- Carefully review your telephone bill every month for unfamiliar charges (they could be monthly or one-time-only charges). Some telephone companies mail out abbreviated bills with few details, but may offer more detailed bills online or upon request.
- Keep an eye out for generic-sounding services and fees listed on your phone bill, like Min. Use Fee, Activation, Member Fee, or Subscription.
- Keep a record of the services you have authorized, even for small charges.
- Don't enter your telephone number on unsecured websites.
- Be on the lookout for unsolicited text messages. A text message from someone you don't know could be a signal that you might be signed up for a service you didn't order.
- Carefully read all forms and promotional materials—including the fine print—before signing up for telephone or other services to be charged on your bill.
- Ask your telephone carrier about any services it may offer that block third-party charges.
- When in doubt, ask questions. If you don't know what a charge listed on your bill is for, ask your telephone company to explain it before you pay it.

More information on cramming can be found on the websites of the Federal Communications Commission and the Federal Trade Commission.



# Preparing for the Pope

## FBI Part of Well-Rehearsed Security Effort



A banner in Washington, D.C. welcomes Pope Francis. The FBI is part of the highly orchestrated security effort surrounding the pope's six-day visit to D.C., New York City, and Philadelphia.

Pope Francis' visit to three major metropolitan areas during his first visit to the United States presents special security challenges. But federal agencies—working closely with state and local law enforcement—have a well-rehearsed template to follow.

The pope's six-day visit to Washington, D.C., New York City, and Philadelphia—which begins September 22—has been designated a national special security event (NSSE) by the Department of Homeland Security (DHS). An NSSE is a significant national or international event

determined by DHS to be a potential target for terrorism or criminal activity. Under the designation, the U.S. Secret Service is placed in charge of event security and the FBI has the lead on collecting intelligence and—should a crisis occur—managing the response. Examples of past NSSEs include State of the Union addresses, party conventions, United Nations General Assembly meetings, inaugural events, and the Winter Olympics and Super Bowl in 2002.

Agencies have been coordinating and training together for months

for the pope's visit, including holding tabletop exercises in each of the cities. Agency leaders briefed the media a week before the pope's arrival after a dry-run exercise in New York City.

"Preparations for events such as this are a cooperative effort," said Diego Rodriguez, assistant director in charge of the FBI's New York Field Office. "No one federal, state, or local agency alone can carry out the measures necessary to secure the event."

While the pope's visit in itself would merit high security, his packed itinerary includes meeting



**Left:** Multiple law enforcement agencies participated in a tabletop exercise at NYPD Headquarters Monday, September 14, as part of security preparations for the pope's arrival.

President Obama at the White House, addressing a joint session of Congress, and speaking at the 70th session of the U.N. General Assembly in New York City—where more than 170 heads of state from around the world are expected to convene.

For the FBI, preparations for the pope's visit come down to relying on the close relationships established during dozens of prior national security events with partner agencies. The Bureau has round-the-clock intelligence operations centers and joint operations centers in all three cities Pope Francis will visit. Liaison agents are embedded with local police at their operations centers and with the Secret Service at their multi-agency coordination center.

"Liaison officers will have collaborated closely to make sure information and intelligence is moving freely," said James Yacone, assistant director of the FBI's Critical Incident Response Group, which is leading the Bureau's efforts during the pope's visit. Yacone said the FBI's national tactical assets—such as the Hostage Rescue Team—are staged to respond if

needed. He described the level of coordination for security as unprecedented.

"This is going to be one of the largest lifts in the nation's history for national security events. There are three major metropolitan areas that are going to all have to seamlessly receive and send off the pope," Yacone said. "That all has to be very skillfully thought out—how we're going to protect him, allow access of the public at different venues, and do it in such a manner that law enforcement can screen as many people as possible to keep it secure."

The heaviest lifting, Yacone said, falls on the uniformed officers who put the plans into action. For weeks now, police departments in D.C., New York, and Philadelphia have put out the word that security will be tight when Pope Francis is in town, with road closures, screening checkpoints, and restrictions on items like bicycles, backpacks and "selfie" sticks.

"From a capacity standpoint, nothing is more important than the participation of our state and local partners," Yacone said. "Neither the

FBI nor the Secret Service could do our jobs effectively without them because they are bringing the capacity."

The agencies involved also rely heavily on the public to increase their capacity to ensure security at the papal-related events and other large gatherings. To submit tips or information about potential threats, visit [tips.fbi.gov](http://tips.fbi.gov).

Procedures for NSSEs were established in 1998 under a presidential directive. The Presidential Threat Protection Act, which codified the Secret Service's role as the lead agency for security, was signed into law in 2000. Since then, participating agencies have jointly managed nearly 50 such events.

Although security can present challenges, Rodriguez said there is a bright side. "While an event this size has the potential to cause inconveniences, I ask you to enjoy this wonderful time...as we prepare for the many historic events that will take place."

#### **Submit Tips**

Agencies involved in ensuring the safety of national security special events—such as Pope Francis' visit to the U.S.—rely heavily on the public to increase their capacity. To submit tips or information about potential threats, visit [tips.fbi.gov](http://tips.fbi.gov).



# Con Man Sentenced in Fraud Case

## Promised Luxury Cars But Rarely Delivered



**Left:** Law enforcement seized this 2008 Mercedes-Benz from Memphis luxury car salesman Michael Brown during the investigation into allegations that Brown was defrauding customers who ordered luxury cars through his company's website.

It's a cautionary consumer tale that's been around forever: In an attempt to get a deal on something that sounds too good to be true, the customer gets the shaft instead.

That's just what happened in the case of a luxury car salesman in Tennessee who used a website to advertise below-market prices on a variety of expensive vehicles. Not only did he not deliver the vehicles ordered by many of his customers, he also kept all or part of the fees they paid him in advance.

The perpetrator's scam, however, eventually caught up with him—as did law enforcement—and this summer, Memphis resident Michael Brown was sentenced to more than six years in federal prison after pleading guilty to mail and wire fraud.

Brown was the sole owner and chief executive officer of Valkry Corporation, a company incorporated in the state of Georgia in 2009 that maintained a website selling luxury cars—it had no showroom. The FBI began looking into Brown's operation in 2011 on the heels of a more than \$1 million civil lawsuit filed by one of his customers—an international luxury car seller based in China—for failing to deliver 16 vehicles the company had paid for by transferring funds into Valkry bank accounts in the U.S.

A significant portion of the investigation, which was conducted by the FBI's Memphis Field Office, was spent analyzing Brown's personal and business financial records. And by reviewing these records, investigators were able to identify some of Brown's victims, conduct interviews with them, and collect additional evidence. For example:

- In late 2012, a luxury car dealership in the United Kingdom placed an order with Valkry for multiple vehicles, with the understanding that the cars would be delivered to them. The company wired more than half a million dollars to a U.S. bank account in Maine under Brown's control. He transferred the funds to his company account in Memphis and then used the money for personal expenses and to buy and trade vehicles which he sold or leased to other customers. Not a dime was spent on behalf of the U.K. company that ordered the vehicles.
- In the summer of 2013, a Tennessee man who had seen Valkry's website negotiated with Brown about the price of a luxury car. The man financed a loan through a credit union and paid Brown for the full amount of the car. Needless to say, the customer never got the car. And Brown used the check for

personal and business expenses.

How was Brown able to carry on the scam for several years? According to the Memphis FBI agent who investigated the case, he was a likeable con man and very smart. To make a money trail harder to follow, he set up a number of bank accounts in different parts of the country, using third parties to open the accounts and to purchase some of his vehicles for him. Said the agent, "He was extremely clever in his movement of funds and assets. I often didn't find out about new accounts he opened until the money was gone."

But eventually, investigators were able to piece together what Brown was doing, which our agent likened to a Ponzi scheme: Brown used money from newer customers to issue partial or full refunds to previous customers, or to purchase cars to sell to other customers, all while using a large portion of his customers' money to support his own lavish lifestyle.

Even the possibility of going to jail didn't slow Brown's criminal activities down: Advised that he was the focus of a federal investigation in July 2012, he continued to ply his trade. For his last criminal act, committed shortly *after* his guilty plea in February 2015, Brown managed to swindle a quarter of a million dollars from a well-known former National Basketball Association player who was looking for a deal on a luxury car.

# Latest Crime Stats Released

## Decrease in 2014 Violent Crimes, Property Crimes

Today, the FBI is releasing the 2014 edition of its annual report *Crime in the United States*, a statistical compilation of offense, arrest, and police employee data reported by law enforcement agencies that participate in the Bureau's Uniform Crime Reporting (UCR) Program. This latest report reveals that the estimated number of violent crimes reported by law enforcement to UCR's Summary Reporting System during 2014 decreased 0.2 percent when compared with 2013 data. And the estimated number of property crimes decreased 4.3 percent from 2013 levels.

Here are some highlights from *Crime in the United States, 2014*:

- There were an estimated 1,165,383 violent crimes (murder and non-negligent homicides, rapes, robberies, and aggravated assaults) reported by law enforcement.
- Aggravated assaults accounted for 63.6 percent of the violent crimes reported, while robberies accounted for 28.0 percent, rape 7.2 percent, and murders 1.2 percent.
- There were an estimated 8,277,829 property crimes (burglaries, larceny-thefts, and motor vehicle thefts) reported by law enforcement. Financial losses suffered by victims of these crimes were calculated at approximately \$14.3 billion.
- Larceny-theft accounted for 70.8 percent of all property crimes reported, burglary for 20.9 percent, and motor vehicle theft for 8.3 percent
- Police made an estimated 11,205,833 arrests during 2014—498,666 for violent crimes, and 1,553,980 for property crimes. More than 73

# 2014

## CRIME in the UNITED STATES

percent of those arrested during 2014 were male.

- The highest number of arrests was for drug abuse violations (1,561,231), followed by larceny-theft (1,238,190) and driving under the influence (1,117,852).

**What's new this year?** For one, the 2014 publication includes the inaugural Federal Crime Data report, which contains traditional UCR data from a handful of federal agencies, as well as FBI arrest data on human trafficking, hate crimes, and criminal computer intrusions.

Also included for the first time in *Crime in the United States* is UCR's second report of human trafficking data submitted by state and local law enforcement.

It is expected that law enforcement participation in data collection for both reports will expand over time, which will help provide a more complete picture of those crimes.

### Message from the FBI Director.

Included in the report is a message from Director James Comey, who said that UCR plans to begin collecting data about non-fatal shootings between law enforcement and civilians, and he encouraged all law enforcement agencies to submit their data about fatal shootings and justifiable homicide data, which is currently collected. Once the FBI begins collecting the expanded data, UCR plans to add a special publication that will focus on law enforcement's use of force in shooting incidents. That report will outline facts about what happened, who was involved, whether there

were injuries or deaths, and the circumstances surrounding the incidents.

Explains Comey, "We hope this information will become part of a balanced dialogue in communities and in the media—a dialogue that will help to dispel misperceptions, foster accountability, and promote transparency in how law enforcement personnel relate to the communities they serve."

In his message, Comey also encourages law enforcement agencies to participate in UCR's National Incident-Based Reporting System (NIBRS), created to improve the quantity and quality of crime data collected by law enforcement by capturing more detailed information on each single crime occurrence.

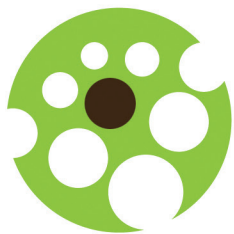
Recently, the International Association of Chiefs of Police—with the Major Cities Chiefs Association, National Sheriffs' Association, and the Major County Sheriffs' Association—released a joint position paper supporting the adoption of the NIBRS to replace the Summary Reporting System. The group says that the NIBRS "provides a more comprehensive view of crime in the United States and offers greater flexibility in data compilation and analysis."

**Looking ahead.** Beginning in January 2016, data collection will begin for the newest UCR Program initiative—animal cruelty offenses—requested by the National Sheriffs' Association and the Animal Welfare Institute.



# Our Shared Responsibility

staysafeonline.org



## National Cyber Security Awareness Month

October is National Cyber Security Awareness Month, administered by the Department of Homeland Security. This is the perfect time of year for individuals, businesses, and other organizations to reflect on the universe of cyber threats and to do their part to protect their networks, their devices, and their data from those threats.

Consider this:

- Within the past year, personally identifiable information has been stolen in a number of significant cyber data breaches, impacting industries like health care, government, finance, corporate, and retail.
- The use of malware by online criminals continues unabated, and of the available intrusion

devices, the “bot” is particularly pervasive, allowing attackers to take control remotely of compromised computers. Once in place, these “botnets” can be used in distributed denial-of-service attacks, proxy and spam services, additional malware distribution, and other organized criminal activity.

- Cyber criminals perpetrate a wide variety of crimes online, including theft of intellectual property, Internet fraud, identity fraud, and any number of financial fraud schemes.
- Sexual predators use the Internet and social media to target the youngest and most vulnerable victims.
- And many criminals use the

so-called “dark web” or “dark market” websites that offer a range of illegal goods and services for sale on a network designed to conceal the true IP addresses of the computers on it.

The FBI—working in conjunction with its many partners at the local, state, federal, and international levels, as well as with industry—takes its own role in cyber security very seriously. That role involves operational efforts—including investigating and disrupting cyber-related national security threats and cyber crimes and collecting, analyzing, and disseminating cyber threat intelligence. It also involves outreach efforts to industry.

Here are just a few examples of how we’re doing all of that:

## Recent Cyber Successes

In May 2015, the owner and operator of the original Silk Road website—an online black market designed to enable its users to buy and sell illegal drugs and other unlawful goods and services anonymously—was sentenced to life in prison. The Silk Road site had previously been taken down by law enforcement in November 2013. In November 2014, the owner and operator of a resurrected Silk Road—Silk Road 2.0—was arrested and charged, and law enforcement took down that site as well, along with dozens of other so-called “dark market” websites. The investigation involved the cooperative efforts of the FBI and numerous local, state, federal, and international partners.

In April 2015, a multi-national law enforcement effort was responsible for taking down a cyber criminal forum that served as a one-stop, high-volume shopping venue for some of the world’s most prolific cyber criminals. Darkode was an underground password-protected meeting place for those interested in buying, selling, and trading malware, botnets, stolen personally identifiable information, credit card information, hacked server credentials, and other pieces of data and software. The FBI was able to infiltrate the forum at the highest levels and collect evidence and intelligence on Darkode members. During the takedown, charges, arrests, and searches involved 70 members and associates around the world.

In April 2015, a coordinated international law enforcement and private sector cyber effort resulted in the takedown of a botnet known as Beebone—a “downloader” that allowed other forms of malware to be installed on victims’ computers without their knowledge or consent. The secondary infections installed by Beebone included software that steals banking logins and passwords as well as fraudulent anti-virus software and ransomware.

## Cyber Tips

As part of National Cyber Security Awareness Month, we will be providing weekly cyber tips through our News Blog and adding them to this page. Check back throughout the month for the latest.

- Cyber Tip #1: Protect Yourself with Two-Factor Authentication (10/05/15)
- Cyber Tip #2: Be Vigilant with Your Internet of Things (IoT) Devices (10/13/15)
- Cyber Tip #3: Defense in Depth for the Every Day User (10/20/15)

- The FBI-led National Cyber Joint Investigative Task Force serves as the national focal point for coordinating cyber threat investigations. The work of the NCJITF includes a national public/private initiative to mitigate the use of botnets and malware by criminals, which has emerged as a global cyber security threat.
- Cyber task forces in all 56 field offices coordinate domestic cyber threat investigations in local communities through information sharing, incident response, and joint enforcement and intelligence actions.
- InfraGard—an information-sharing and analysis effort with private sector partners who own, operate, and hold key positions

within some 85 percent of the nation’s critical infrastructure—equips its members to identify and mitigate vulnerabilities, develop incident response plans, and enact security best practices.

- The Internet Crime Complaint Center (IC3) accepts online submissions for Internet-related crime complaints, often involving fraudulent claims to consumers. These complaints can not only lead to culprits getting caught, but also help identify regional, national, or international trends to educate the public about constantly evolving cyber threats and scams.
- The FBI’s Safe Online Surfing website, an online program that promotes cyber citizenship by educating young students in the

essentials of online security in an effort to help protect them from child predators, cyber bullies, malware, a multitude of schemes, and other dangers on the Internet.

The Bureau will continue to work jointly with our national security and law enforcement partners to address threats to the nation’s cyber security from nation-states, terrorist organizations, transnational criminal enterprises, and child predators. But government can’t do it alone—assistance and vigilance from the public is vital.

Stay tuned to our website during the month of October—we’ll be providing you with tips that will help keep your families and your businesses safe from cyber criminals.



# Insurance Broker Sentenced for Fraud

## Hundreds of Companies Victimized in Multi-State Scheme

More than 800 commercial trucking companies in nearly a dozen states paid Atlanta-area insurance broker John Paul Kill approximately \$3.7 million in premiums from 2013 to mid-2014 to purchase insurance that protected their livelihoods: their cargo and the trailers that carried it.

There was only one problem—for the most part, Kill didn't purchase the insurance requested by his customers. Investigators with Georgia's Insurance Commissioner's Office discovered that Kill pocketed the premiums for his personal use.

Once Georgia officials realized the extent of Kill's activities—millions of dollars in stolen premiums from customers in multiple jurisdictions—the office requested the assistance of the FBI. And as a result of the ensuing joint investigation, Kill pled guilty in federal court earlier this year to the nationwide cargo insurance scam. This past August, he was sentenced to four years in a federal prison and was also ordered to pay \$1.23 million in restitution to his victims.

How did the scheme work?

In 2013, Kill, through his company, Appeals Insurance Agency (AIA)—which was actually housed in the basement of his home—began offering cargo insurance. He advertised his services mostly through word of mouth and by making cold calls to commercial trucking companies. Kill would solicit insurance agents to write policies for trucking companies and then, in his capacity as a broker, would claim to “bind” the policies written for those companies to recognized insurance companies, including Lloyd's of London. In the insurance industry, binding

coverage serves as an official agreement between the insurance provider and the insured party to provide insurance coverage.

For a small percentage of his clients, Kill bound cargo insurance policies through insurance companies that actually offered less extensive coverage than what the trucking companies thought they had purchased. But most of his clients received no policies at all—despite the premium payments they paid to Kill.

***“This case was about theft and greed. Mr. Kill displayed a complete disregard for his client companies, leaving them legally and fiscally vulnerable while allowing them to believe that they had appropriate insurance coverage.”***

In addition to using the premiums sent to him by the trucking companies for his own benefit, Kill used a portion of the funds to pay off insurance claims that were filed with his office. Since most of his customers had no actual insurance coverage, he paid their claims so he wouldn't raise their suspicions—he wanted to prolong the life of his illegal scheme for as long as possible.

At one point, though, a concerned insurance agent sent Lloyd's of London a copy of a contract supposedly bound by John Paul Kill but which was actually fraudulent. Lloyd's then contacted Georgia's Insurance Commissioner's Office to file a complaint. That office investigated, and subsequent search warrants uncovered bank ledgers

showing that Kill, through AIA, deposited the illegal proceeds of his fraud into his own personal bank accounts. Kill later admitted to putting insurance premium checks into his accounts and also to creating insurance policy cover sheets for insurance agents and customers to make them believe they had purchased cargo theft insurance.

In addition to the actual trucking companies, Kill's victims included the insurance agents and insurance agencies who wrote the policies—many were significantly affected by Kill's actions in terms of monetary losses, harm to their reputations, and civil lawsuits filed by the trucking companies.

At the time of Kill's guilty plea, FBI Atlanta Special Agent in Charge J. Britt Johnson said, “This case was about theft and greed. Mr. Kill displayed a complete disregard for his client companies, leaving them legally and fiscally vulnerable while allowing them to believe that they had appropriate insurance coverage. The FBI is pleased with the role it played in bringing this case forward for prosecution and holding Mr. Kill accountable for his actions.”

And if a prison term and an order to pay more than a million dollars in restitution weren't bad enough for John Paul Kill, the state of Georgia also revoked his license to sell insurance.

Special thanks to our colleagues in Georgia's Insurance Commissioner's Office, whose expert investigative work laid the foundation for this successful federal prosecution.

# Identity Theft

## Fake Hospice Nurse Treated More Than 200 Patients

Imagine the emotional difficulty of arranging in-home hospice care for a terminally ill family member. Now imagine learning after the fact that your loved one had been cared for not by a nurse but by a medical imposter.

That is exactly what happened in more than 200 cases in the Dallas/Fort Worth area over nearly a three-year period when a woman who had stolen the identity of a registered nurse used those credentials to gain employment with multiple hospice companies.

“Jada Necole Antoine had absolutely no nursing experience or medical training,” said Special Agent Brian Marlow, who investigated the case out of the FBI’s Dallas Division. “The thought of having someone who is not a nurse taking care of your parent or loved one is not only criminal, it is morally outrageous.”

The Bureau’s investigation began in 2013 as a result of a local traffic stop in Texas. When the patrol officer asked for identification, Antoine produced her own driver’s license, and it turned out there was a warrant for her arrest on another matter. She also had other identification in the car—including documents belonging to the victim nurse—along with a number of medical records. That information was forwarded to the Medicare Fraud Strike Force team in Texas, which consists of the FBI, the Department of Health and Human Services, the Texas State Attorney General’s office, and local law enforcement. The strike force is part of a larger, nationwide effort aimed at combating health care fraud and abuse.

As the strike force team began to investigate the paperwork found



in Antoine’s car, “we learned about the hospice companies Antoine had been associated with,” Marlow said. “In all, we found eight different hospices she had worked for using the nurse’s stolen identity.”

During the time she was carrying on this fraud—from approximately January 2009 through April 20, 2012—Antoine was paid more than \$100,000 from the various companies who unwittingly employed her. She had direct responsibility for patient care and submitted documents to the hospice companies that falsely indicated care was provided by a registered nurse. Those false statements caused the hospice companies to submit false claims to Medicare and Medicaid totaling approximately \$800,000.

Antoine victimized 243 hospice patients by depriving them of legitimate health care from a properly licensed individual, Marlow said. Court records show

that Antoine treated patients who were mentally ill, comatose, asleep, and otherwise unresponsive to sound and touch, and in those instances, she made her own assessments of the patient’s pain and comfort levels, digestive function, and breathing.

She also had access to patients’ medical charts and detailed personal information, which, said Marlow, “was greatly concerning because of her history of identity theft crimes.”

With investigators on her trail, Antoine fled Texas but was apprehended in Georgia in 2014 and charged with fraud and identity theft. She pled guilty, and this past August, a federal judge sentenced the 34-year-old to four years in prison.

“Many of the patients she allegedly cared for were completely at her mercy,” Marlow said. “Now that she is behind bars,” he added, “she will not be able to victimize anyone else.”



# Operation Cross Country

## Recovering Victims of Child Sex Trafficking

Operation Cross Country, a nationwide law enforcement action that took place last week and focused on underage victims of prostitution, has concluded with the recovery of 149 sexually exploited children and the arrests of more than 150 pimps and other individuals.

The FBI, in partnership with local, state, and federal law enforcement agencies and the National Center for Missing & Exploited Children (NCMEC), conducted the annual action—the ninth and largest such enforcement to date—as part of the Bureau’s Innocence Lost National Initiative.

“Our mission is to protect the American people—especially our children—from harm,” said FBI Director James Comey.” When kids are treated as a commodity in seedy hotels and on dark roadsides, we must rescue them from their nightmare and severely punish those responsible for that horror. We simply must continue to work with our partners to end the scourge of sex trafficking in our country.”

“Human trafficking is a monstrous and devastating crime that steals lives and degrades our nation,” said Attorney General Loretta

Lynch. “As a result of the FBI’s outstanding coordination and exemplary efforts alongside state and local partners during Operation Cross Country, more children will sleep safely tonight, and more wrongdoers will face the judgment of our criminal justice system.”

Since its creation in 2003, the Innocence Lost program has resulted in the identification and recovery of approximately 4,800 sexually exploited children. And prosecutors have obtained more than 2,000 convictions of pimps and others associated with these



An officer with the Alexandria (Virginia) Police Department monitors an undercover sting operation in a hotel room during Operation Cross Country.



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/occ9](http://www.fbi.gov/occ9).

trafficking crimes, including at least 15 cases that have resulted in life sentences.

This year's enforcement action, coordinated through 73 of the FBI's Child Exploitation Task Forces—which include federal, state, and local law enforcement agencies—was conducted nationwide in 135 cities. More than 500 law enforcement officials took part in sting operations in hotels, casinos, truck stops, and other areas frequented by pimps, prostitutes, and their customers. The youngest recovered victim was 12 years old.

“We are proud to partner with the FBI and provide support to both law enforcement and victim specialists in the field as they work to locate and recover survivors of child sex trafficking,” said Linda Krieg, NCMEC's acting chief executive officer. “The number of children recovered and pimps arrested in this year's operation highlights the importance of these efforts today and every day in protecting our children.”

During Operation Cross Country, nearly 100 victim specialists from the FBI's Office for Victim Assistance provided on-scene

services to recovered young victims. Services included crisis intervention as well as resources for basic needs such as food, clothing, shelter, and medical attention.

“From an investigative standpoint, Operation Cross Country targets the individuals and criminal enterprises responsible for the commercial sex trafficking of children,” said one of the Bureau's victim specialists. “But our main goal is to provide support and services for these young victims—to help stabilize them and get them moving forward in a positive direction.”



Operation Cross Country actions in Alexandria, Virginia. Operation Cross Country is a weeklong, FBI-led enforcement action to address commercial child sex trafficking throughout the United States.



Following Operation Cross Country, digital billboards such as this were featured nationwide as part of the FBI's continuing efforts to stop the sex trafficking of children.



# Race and Law Enforcement

## Director Urges Closer Ties Between Police, Communities



FBI Director Comey (center) joins Cleveland Police Department Chief Calvin Williams (left) and Cuyahoga County Sheriff Clifford Pinkney (right) at a forum in Cleveland, Ohio on October 15, 2015.

FBI Director James Comey is continuing to urge police agencies and their constituents—particularly in communities of color—to take steps to better understand one another to help stem what he sees as a growing disconnect.

“I imagine two lines,” Comey said Thursday during a forum at Cuyahoga Community College in Cleveland, Ohio that included local law enforcement, community leaders, prosecutors, and high school students. “One [line] is us in law enforcement and the other is the folks we serve and protect. And I think those two lines are arcing away from each other.”

The Director’s remarks echoed a speech he delivered on the subject of race and law enforcement last February at Georgetown University in Washington, D.C. The speech

followed lethal police encounters that occurred the previous summer in Ferguson, Missouri and New York City—sparking protests and intense public debate—and the apparent retribution killings of two uniformed New York Police Department officers in December 2014.

At the time, Comey suggested his remarks were only the beginning of a broader and much-needed exchange on the subject. “These are only conversations in the true sense of that word if we are willing not only to talk but to listen, too.”

In the months since then, the Director has continued to talk on the subject and FBI field offices around the country have reached out to their own communities to further that conversation as well.

In Cleveland, where violent crime rates have risen dramatically

this year, Director Comey joined Cleveland Police Chief Calvin Williams, Cuyahoga County Sheriff Clifford Pinkney, and more than 200 members of the local community to talk and to listen.

“I’m here because I think Cleveland is a place of great pain that is in a way illustrative of that crisis of those bending arcs,” Comey said.

It was in Cleveland that a 12-year-old African-American boy, Tamir Rice, was fatally shot by a police officer while holding a pellet gun in November 2014. The city is implementing a federal agreement following a Department of Justice determination last year that city police officers too often used excessive force and violated people’s civil rights. A provision of the settlement is to better train officers in community engagement.



Cleveland Police Chief Calvin Williams mingles with students from a local high school following a forum on race and law enforcement.

During the question-and-answer-style forum, moderated by FBI Cleveland Special Agent in Charge Stephen Anthony, the panelists agreed that a major step forward would be for police to get out of their cars and get better acquainted with people in their communities. But the hard work has to be shared, they said.

“For law enforcement to be successful—to make a better community—we need your help,” Sheriff Pinkney told attendees, including some 40 young students seated in the front rows. “We need your support, whether it’s publicly or anonymously—we need you to be a part of this team.”

Comey said the answer to finding more common ground was “unscientific.”

“It’s simply understanding that it’s hard to hate up close,” Comey said.

“We must see each other more clearly.”

In the audience, Ryan Hurley, a humanities teacher at St. Martin de Porres High School, listened with interest, alongside a dozen of his students.

“We’re having this conversation in our classes, we’re having this conversation in our school because it’s important,” Hurley said following the event. “I think the big takeaway is that it’s sort of a shared responsibility. And they’re okay taking on that responsibility if they feel like they have trust in the people at the top.”

After the forum, Hurley asked students what they thought.

“Their first response was, ‘They seem a lot different here than they do on the news.’”

Cleveland Police Chief Williams was optimistic that things

were beginning to change. His department, along with the FBI, recently held a “Safety in Your Sanctuary” program for about 40 local clergy members. Another recent community event focused on police use of force.

“I think that right now, this moment, we’re at a point where we’re going up,” Williams said. “I think we’re at a point where people are actually coming together to really talk sensible solutions about things that are happening.”

The Director said Cleveland was an ideal location to continue the discussion of race and law enforcement. “This is a place of tremendous promise,” he said. “Given the quality of the leadership you have here and the folks here in this room, you actually have the best chance of arcing those lines back together and showing this country how it can be done.”



# In the Line of Duty

*Law Enforcement Officers Killed and Assaulted, 2014 Report Released*



On May 29, 2014, a 42-year-old trooper with the New York State Police made a traffic stop on an interstate highway north of Binghamton. The veteran trooper parked behind the stopped car and approached the driver's side window. In that fleeting moment, a truck traveling in the same direction at about 90 miles per hour suddenly swerved, sideswiping the car and striking the trooper, killing him instantly. The truck's driver, a 60-year-old male with a criminal record, admitted after his capture that he intentionally veered to hit the trooper.

The chilling account of the unprovoked attack is just one of dozens of detailed narratives recounting the felonious deaths of law enforcement officers in the United States in 2014. The accounts are a central component of the latest *Law Enforcement Officers Killed and Assaulted* (LEOKA) report, issued

today, which shows that 96 law enforcement officers were killed in the line of duty last year—51 as a result of felonious acts and 45 in accidents. The annual report, released by the FBI's Uniform Crime Reporting (UCR) Program, also shows that 48,315 officers were victims of line-of-duty assaults in 2014.

In addition to the narratives, the online-only report includes comprehensive data tables that provide a closer look at the incidents: officer profiles, circumstances, weapons, locations, and identified suspects.

The felonious deaths of the 51 officers—all males—occurred in 24 states and Puerto Rico. The figure represents a significant increase over the number that occurred in 2013, when 27 officers were killed, but is lower than the numbers from 2009 (56 officers) and 2005 (55 officers).

Left: This chart provides a breakdown of the circumstances under which 51 officers were feloniously killed in the line of duty in 2014; an additional 45 officers were killed in accidents during the same time period.

Among the report's findings:

- The average age of the officers who were feloniously killed was 39, and they had served for an average of 13 years.
- Offenders used firearms to kill 46 of the 51 victim officers: 33 were slain with handguns, 10 with rifles, and three with shotguns.
- 59 alleged assailants (54 of them males) were identified in connection with the line-of-duty deaths; 50 had prior criminal arrests.
- 39 of the officers feloniously killed with firearms were wearing body armor at the time of the incidents.
- The largest percentage (30.8) of assaults on police officers occurred while they were responding to disturbance calls.

The LEOKA publication contains data on duly-sworn city, university/college, county, state, tribal, and federal law enforcement officers. The information in the report comes from various sources: the law enforcement agencies participating in the UCR Program, FBI field offices, and several non-profit organizations, such as the Concerns of Police Survivors and the National Law Enforcement Officers Memorial Fund.

In addition to collecting details about the critical aspects of fatal confrontations and assaults, the FBI's LEOKA Program conducts extensive research on the data that eventually gets incorporated into officer safety awareness training the FBI provides for partner agencies.

# Operation Northern Spotlight

## American-Canadian Partnership Combats Human Trafficking

The FBI joined law enforcement officials from across Canada in Toronto yesterday to announce the results of Operation Northern Spotlight, a human trafficking investigation that led to the recovery of 20 sexually exploited juveniles and the arrests of numerous individuals.

The Canadian operation—carried out by 40 police agencies and hundreds of law enforcement officers—was conducted as a parallel action with the FBI's Operation Cross Country, the results of which were announced earlier this month.

“Human trafficking investigations are complex and labor intensive, but entirely necessary,” said Scott Tod, deputy commissioner of the Ontario Provincial Police (OPP). He noted that human trafficking victims are often from susceptible populations, including immigrants, migrant workers, and at-risk youth. “And human trafficking victims rarely identify themselves to authorities,” he said.

“Human trafficking is a very serious criminal threat that often targets the most vulnerable—our children,” added Joseph Campbell, assistant director of the FBI's Criminal Investigative Division. The collaboration between U.S. and Canadian law enforcement to fight trafficking, he explained, is essential.

Operation Cross Country is part of the FBI's Innocence Lost National Initiative. Since its creation in 2003, the Innocence Lost program has resulted in the identification and recovery of approximately 4,800 sexually exploited children. And prosecutors have obtained more than 2,000 convictions of



Law enforcement officials from across Canada announced the results of Operation Northern Spotlight, a human trafficking investigation carried out earlier this month in conjunction with the FBI's Operation Cross Country efforts. Joseph Campbell (center), assistant director of the FBI's Criminal Investigative Division, took part in the press conference, held in Toronto on October 22, 2015.

pimps and others associated with these trafficking crimes.

During last year's Operation Cross Country, Campbell said, “I met with our Canadian law enforcement partners, and we agreed that this mission was so critical and important that it should be a unified effort between our two countries.”

***“It is vitally important that we continue to mobilize to raise awareness about human trafficking and to enhance public safety at the community level.”***

That collaboration resulted in parallel enforcement actions that took place across the U.S. and Canada in early October, with both countries sharing intelligence and best practices to run successful operations that led to the recovery of child victims from truck stops, hotels, clubs, and casinos. The Canadian effort led to charges against 47 individuals and the

recovery of victims who were mostly under the age of 19—some as young as 14.

Yesterday's press conference in Toronto included law enforcement personnel from OPP, the Royal Canadian Mounted Police, Ottawa Police Service, and numerous other Canadian law enforcement agencies. Also on hand were representatives from a child advocacy center and a recovered victim of the sex trade who now advocates on behalf of those who are trafficked and sexually exploited.

“It is vitally important that we continue to mobilize to raise awareness about human trafficking and to enhance public safety at the community level,” Tod said.

Campbell agreed. “Operation Cross Country and Operation Northern Spotlight are so important because they maximize the impact in combating the threat and they draw attention to this serious problem. I am proud to stand here today with my Canadian partners.”



# Symposium Facilitates Research on Lawful Interrogations

Event Sponsored by Government's High-Value Detainee Interrogation Group

"The rule of law in the Constitution is our spine, it's who we are, it's part of our fiber...and we want humane, effective, lawful encounters with every human being."

Those words were spoken last week by FBI Director James Comey as he was discussing the efforts of the U.S. government's High-Value Detainee Interrogation Group (HIG) during the HIG's fifth annual research symposium, held October 23 at the National Academy of Sciences in Washington, D.C.

Comey, who briefed symposium participants on the evolving terror threat, also said that the HIG's work "is valuable beyond national security cases" and that the group's research and training efforts benefit

law enforcement interviewers as well.

The HIG, established in 2009, brings together personnel from the U.S. Intelligence Community to conduct interrogations that strengthen national security and that are consistent with the rule of law. But in addition to its operational role in eliciting accurate and actionable intelligence from high-value terrorism subjects, the HIG plays another vital role as well—serving as the government's focal point for interrogation best practices, training, and scientific research. And during its yearly research symposium—coordinated by the Center for Law & Human Behavior at the University of Texas at El Paso—scientists from the U.S. and abroad who work with the HIG have the opportunity

to share with policy makers and intelligence professionals groundbreaking research that can impact the effectiveness of interview and interrogation methods.

All HIG-sponsored research is unclassified—researchers who work with the HIG are free to publish their findings, and most do. At this year's symposium, participants presented research on topics like the dynamic nature of interrogations, the challenges of interviewing through interpreters, the use of rapport rather than tough tactics, negotiations across cultures, subtle elicitation approaches, and priming disclosure and cooperation.

**Background on the HIG:** The director of the HIG is an FBI representative and is assisted



Director Comey addresses the audience at the High-Value Detainee Interrogation Group's fifth annual research symposium, held October 23, 2015 in Washington, D.C.

by two deputies—one from the Department of Defense and the other from the Central Intelligence Agency. Full-time HIG members are augmented part-time by HIG-trained professionals from FBI field offices and other U.S. Intelligence Community agencies.

HIG responsibilities fall under three primary areas, all of which feed into one another:

- **Interrogations:** The HIG deploys expert Mobile Interrogation Teams (MITs) to collect intelligence that will prevent terrorist attacks and protect national security. Since the HIG's creation, MITs have been deployed within the U.S. and abroad. Deployment teams generally consist of a team leader, interrogators, analysts, subject matter experts, linguists, and other personnel as needed. HIG interrogators are chosen for—among other attributes—their extensive interviewing and interrogation experience and their willingness to adapt to evolving interrogation techniques based on the latest scientific research.
- **Research:** The goal of the HIG's research program is to study the effectiveness of interrogation approaches and techniques by identifying and validating existing techniques that work—and by developing new lawful techniques that may work even better. The HIG identifies research gaps in the interrogations field and commissions research products to fill in these gaps. To carry out the research, the HIG contracts with Ph.D.-level scientists from all over the world known for their expertise in interrogations and other related fields. Since its founding, the HIG has funded nearly 80 interrogation research projects, some of which have covered interviews with expert interrogations interrogators, social influence tactics, the impact of interpreters, the cognitive interview, the strategic use of evidence, and science-based methods of detecting deception. **A side note:** All HIG research is done in complete compliance with international laws and U.S. laws concerning the protection of human research subjects.
- **Training:** The HIG works to develop and disseminate best practices for training purposes for its own interrogators and part-time personnel and for other U.S. Intelligence Community and law enforcement partners

and allies abroad. Over the past year, HIG trainers—who are FBI-certified training instructors—have worked with more than 500 students from multiple agencies, including 90 foreign partner participants. And some of the HIG's interrogation techniques have been added to the curricula of the Department of Defense's human intelligence training facility in Arizona and the Federal Law Enforcement Training Centers in Georgia, among others. HIG interrogations are primarily terrorism-related, but the lawful interrogation techniques can also be used when questioning criminal suspects, which is why we share best practices with and conduct training sessions for select state and local law enforcement partners.

#### **Has the HIG been effective?**

According to HIG Director Frazier Thompson, "Much of our operational work is necessarily classified, but I can tell you this—as a result of the HIG, plots to harm the U.S. and its allies have been disrupted, dangerous people have been put behind bars, and gaps in U.S. intelligence collection have been bridged."

#### **The Truth About the HIG**

There are several misconceptions about the High-Value Detainee Interrogation Group (HIG) that we'd like to clear up. Here is the truth:

- *The HIG does NOT use torture.* HIG personnel do not engage in any unlawful interrogation practices—they use authorized, lawful, non-coercive techniques based on the best science available that are designed to elicit voluntary statements and that do not involve the use of force, threats, or promises.
- *The HIG does NOT select its own intelligence targets.* With U.S. intelligence requirements in mind, targets are nominated by a U.S. intelligence agency and must be approved by appropriate partner agency leadership.
- *The HIG is NOT the FBI.* Even though the HIG is administratively housed within the FBI, it is a multi-agency organization whose principal function is intelligence gathering—not law enforcement—and it is subject to oversight through the National Security Council, the Department of Justice, and Congress. That being said, the actions of HIG teams are carefully documented and evidence preserved in the event of a criminal prosecution, and its members are prepared to testify in court if necessary.



# Financial Fraud

## Inside the Investigation of a Las Vegas Construction Boss



During one phase of the lengthy investigation into Leon Benzer and his associates, an undercover operative received a \$20,000 bribe in a Las Vegas parking lot from one of the subjects in the case—while the FBI secretly recorded the transaction.

When a federal judge sentenced former Las Vegas construction boss Leon Benzer to nearly 16 years in prison in August, it marked a final chapter in a \$58 million fraud scheme that took investigators nearly a decade to unravel.

Over a period of many years, Benzer brazenly sought to gain control of numerous condominium homeowners associations (HOAs) in the Las Vegas area to secure lucrative construction and other contracts for himself and additional conspirators. To date, 44 individuals, including numerous state officials, have been convicted of crimes in connection with the fraud—which has been described as one of the largest public corruption cases in Nevada history.

“This case represented an incredibly complicated financial fraud with a significant public corruption component,” said Special Agent Michael Elliott, who spent nearly eight years working on the investigation from the FBI’s

Las Vegas Division. “It involved so many people over so long a period of time, it was like an intricate spider web of crime that kept expanding.”

The scheme was nothing if not grandiose. In attempting to control dozens of Nevada HOAs between approximately 2002 and 2009, Benzer, an attorney, and other conspirators recruited straw buyers to purchase condominiums and then secure positions on HOA boards of directors. Benzer rigged HOA board elections and paid board members to take actions favorable to his interests—including hiring his co-conspirator’s law firm to handle construction-related litigation and awarding profitable construction contracts to Benzer’s company, Silver Lining Construction.

Benzer manipulated and bribed HOA boards in a variety of ways—he often claimed he had local judges and law enforcement in his pocket; in other cases, he

fooled unwitting homeowners into thinking his actions were legitimate and they were simply making wise investment choices.

In September 2008, investigators executed a search warrant—one of nine that would take place during the investigation—and found that Benzer was in the process of targeting well over 20 different HOAs for illegal takeovers. “There were boxes and boxes of folders with information about different HOAs,” Elliott said. “He was deliberately attempting to identify board members along with other information to target what he believed were HOAs vulnerable to takeover through bribery, extortion, or whatever illegal means could be used.”

One of the HOAs had more than 700 units, with each owner paying community fees, Elliott said. “In some cases, HOA boards had operating budgets larger than some small Nevada cities. There was lots of money at stake,” he added.

The FBI, along with investigators from the Las Vegas Metropolitan Police Department and Internal Revenue Service-Criminal Investigations, used a variety of investigative techniques—including confidential sources, multiple undercover operatives, and forensic accountants—and conducted hundreds of interviews to piece together the extent of the crimes committed by Benzer and his co-conspirators.

In January 2015, Benzer pled guilty to multiple counts of conspiracy to commit mail and wire fraud and tax evasion. In addition to his 188-month jail term, he was ordered to pay more than \$13 million in restitution. “This was a very sophisticated scam that evolved over time and generated millions of dollars for Benzer,” Elliott said, adding that when Benzer was riding high, the charismatic fraudster employed “an

army of lawyers, had bodyguards, and had an entourage that included three armored SUVs. He had no problem spending money to maintain his lavish lifestyle.”

But like many high-flying scam artists, it was only a matter of time before Benzer was brought to justice. “Now he is in jail and penniless,” Elliott said. “He has nothing.”



Evidence in the case against Leon Benzer included a \$20,000 cash bribe that was concealed in this baby wipes container.



# Public Corruption Fugitive Extradited to U.S.

## State Official Returns to Face Justice



Public corruption is the FBI's top criminal priority, and the recent return of a convicted public official who had fled overseas demonstrates the lengths the Bureau will go to ensure that those who betray the public trust are brought to justice.

The investigation into Amer Ahmad, former deputy treasurer for the state of Ohio, began with allegations of corruption involving that office's awarding of lucrative contracts to manage state-owned securities. It ended with guilty pleas and subsequent federal prison sentences for Ahmad and his three co-conspirators, but Ahmad was sentenced in absentia because he had fled to Pakistan, the birthplace of his parents.

**How it all started.** The Ohio treasurer is the state's cash manager and chief investment officer with the duty of collecting

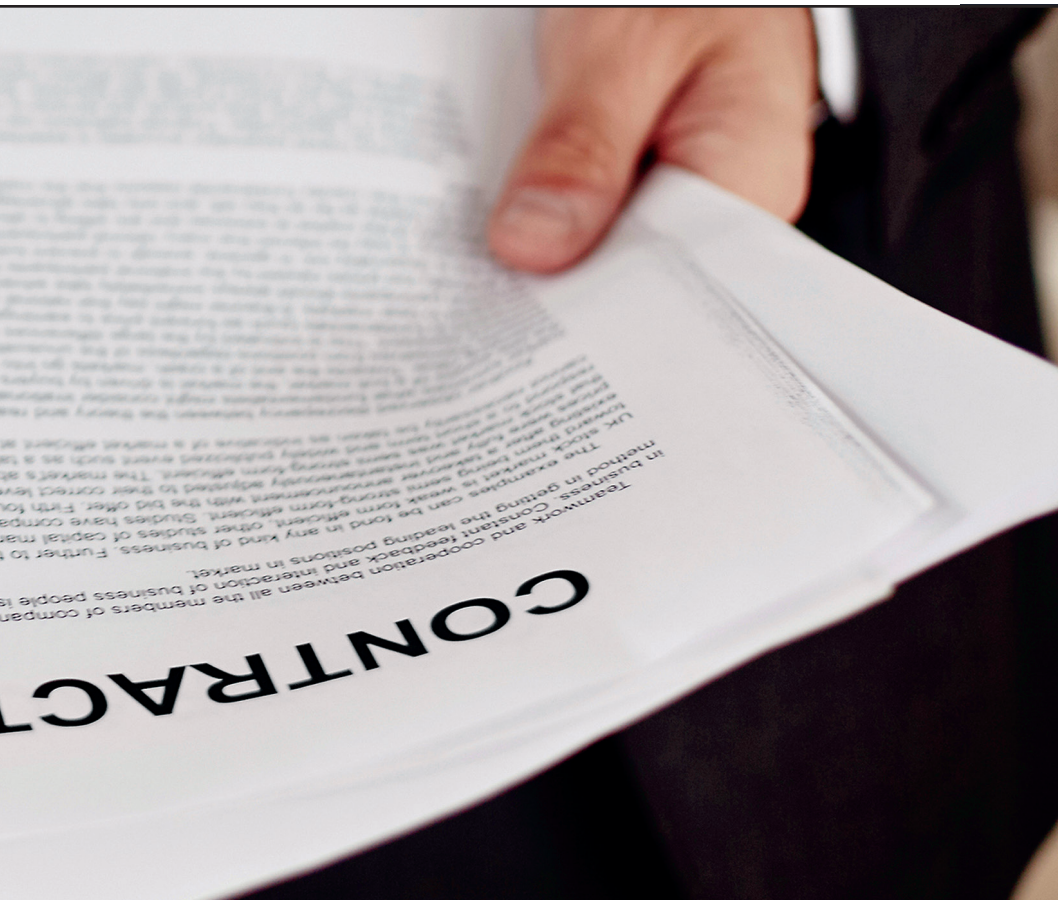
and overseeing public funds, and the treasurer's office has an investments department responsible for actively handling the state's multi-billion investment portfolios. Amer Ahmad became the chief financial officer for the treasurer's office in 2008, and the following year, he was also appointed deputy treasurer.

But by 2010, following allegations of corruption with the treasurer's office, the FBI's Columbus Resident Agency opened a case (and was later assisted by its partners at the Ohio Bureau of Criminal Investigation—members of the newly formed Central Ohio Public Corruption Task Force).

As the case unfolded, investigators identified Ahmad and three other individuals as the primary players in the corruption scheme. Ahmad's co-conspirators included:

- Douglas Hampton, a high school classmate of Ahmad's who worked as a broker and financial adviser (and in whose financial firm—Hampton Capital Management—Ahmad and his wife maintained a personal investment account);
- Joseph Chiavaroli, a Columbus businessman who co-owned a landscaping company with Ahmad; and
- Mohammed Noure Alo, a close friend of Ahmad's who was a lawyer in a Columbus-based law firm and registered as a lobbyist in the state of Ohio.

**The scheme.** From January 2009 to January 2011, Ahmad used his position to direct official state business to the financial firm run by Hampton in return for more than \$500,000 in bribe payments. Records showed that Hampton



### Partnership Against Corrupt Officials Pays Off in Central Ohio

In 2013, to more effectively address corruption in the state capital of Columbus, the FBI created the Central Ohio Public Corruption Task Force. In addition to the Bureau, the task force includes numerous agents from the Ohio Bureau of Criminal Investigation and investigators from the U.S. Department of Transportation-Office of Inspector General, U.S. Department of Labor-Office of Inspector General for Labor Racketeering and Fraud, and Internal Revenue Service-Criminal Investigation.

In its short existence, the task force has been extremely successful. Besides assisting with the convictions of Amer Ahmad and his co-conspirators, it has worked toward convictions of four members of the Ohio General Assembly and numerous corrupt law enforcement officers, lobbyists, public officials, and businesspersons.

Capital Management became an approved Ohio treasurer's office broker in 2009 through a process personally overseen by Ahmad and had received the most trades—360—of any broker for the state of Ohio in 2009 and 2010. Hampton made approximately \$3.2 million in commissions from those trades.

Ahmad conspired with Chiavaroli to conceal the illegal payments from Hampton by passing them through the accounts of their landscaping company. (In late 2009, Chiavaroli had executed a bill of sale transferring 46 percent ownership of his landscaping company to Ahmad.)

Hampton also funneled a number of payments to Ahmad through Alo, who profited from the scheme by keeping some of the money himself.

Investigators were able to obtain evidence of the corruption—and of the conspiracy—from a variety of sources, including e-mails, financial records, and interviews.

All four subjects were indicted on corruption charges in August 2013. At the time of his indictment, Ahmad had already left his job in Ohio to take another government position, this one with the city of Chicago. After guilty pleas by Hampton, Chiavaroli, and Alo, Ahmad pled guilty in December 2013.

**The flight.** In April 2014, while awaiting sentencing, Ahmad fled the country and eventually flew to Pakistan. But upon his arrival at the airport, he was arrested by Pakistani authorities for attempting to enter the country using false documentation and taken into custody.

Immediately upon discovering that Ahmad was in Pakistan, U.S. authorities began extradition proceedings. In the meantime, in December 2014, Ahmad was sentenced—without physically being in court—to 15 years in federal prison. His co-conspirators also received prison terms.

And by August 2015, Ahmad was on another plane—this time in the company of FBI agents and U.S. marshals—bound for Ohio.

Corrupt public officials can undermine our security, our safety, and public trust and confidence in our government, while wasting billions of dollars along the way. That's why the FBI will continue to investigate these types of cases so strenuously.



# Navy Engineer Sentenced for Attempted Espionage

## Passed Information on Latest Aircraft Carrier to Undercover Agent

In the fall of 2014, civilian engineer Mostafa Ahmed Awwad provided schematics of the U.S. Navy's newest nuclear aircraft carrier—the USS *Gerald R. Ford*—to an individual he thought was an Egyptian intelligence officer. At the time, Awwad was an employee of the Norfolk Naval Shipyard in Portsmouth, Virginia, and had access to naval nuclear propulsion information.

His actions could have potentially compromised the safety of some 4,000 American sailors who will be serving on the USS *Gerald R. Ford* after it joins the fleet of Navy vessels sometime next year—and the security of our nation in general. Fortunately, Awwad's Egyptian contact turned out to be an undercover FBI agent. And last month, Awwad was sentenced to 11 years in prison after pleading

guilty earlier this year to attempted espionage.

After joint investigative efforts between the FBI and the Naval Criminal Investigative Service (NCIS), an undercover Bureau agent reached out to Awwad by telephone in September 2014 and, speaking Arabic, asked to meet with him. Without asking any questions, Awwad agreed.

The pair met the next day in a park in nearby Hampton, Virginia. During the meeting, which was audio and video recorded, our agent identified himself as being a representative of the Egyptian government. Awwad told our agent that he wanted to use his position at the Norfolk Naval Shipyard to obtain military technology for use by Egypt, including the designs of the USS *Gerald R. Ford*. The two

discussed how they would remain in future contact—through coded e-mail communications and dead drops in a concealed location in the park.

In October 2014, at Awwad's request, the two men met in a hotel room in Norfolk. During that meeting, which was also recorded, Awwad gave the undercover agent electronic copies of schematic drawings of the USS *Gerald R. Ford*, which clearly contained numerous markings warning against disseminating the information publicly. Awwad said he planned to obtain additional information concerning the tools and the technology necessary to build the carrier and also pointed out on the schematics vulnerable areas where a strike could cause an explosion significant enough to sink the carrier.



The dead drop area in a Virginia park that was used by Navy civilian engineer Mostafa Ahmed Awwad to pass sensitive information on the USS *Gerald R. Ford*, a new aircraft carrier currently under construction.



During this same meeting, Awwad described for the agent his plans to circumvent Navy computer security by installing software on his restricted computer that would enable him to copy documents without triggering a security alert. He also asked for money to buy a pinhole camera, which he intended to use throughout the shipyard to take pictures of restricted material.

And finally, Awwad told the agent that going forward, the two would communicate primarily through e-mail. The engineer, admittedly fearful of being caught by the FBI, instructed the agent to create 24 fake e-mail accounts that should be used only once and then deleted. He also asked for an escape plan in the event his activities were detected by the FBI.

Over the next month or so, Awwad and the undercover agent e-mailed numerous times and met again in a hotel. Awwad was also recorded servicing the dead drop location in the Hampton park, picking up \$3,000 left by the agent at Awwad's request so he could purchase a laptop and dropping off an external hard drive of additional schematic drawings and two photos to be used for producing a fraudulent passport.

All the while, there was no doubt that Awwad understood that the "Egyptian representative" he was dealing with would be passing the stolen information to the Egyptian government.

Why did he do it? Awwad told our undercover agent that he was motivated to use his position to steal nuclear and defense secrets from the U.S. to aid Egypt in building a more robust defense. And at one point, he said he wanted to go to Egypt to meet



This surveillance photo shows Mostafa Ahmed Awwad, left, meeting with an FBI undercover agent he believed was an Egyptian intelligence officer.

personally with high-ranking intelligence and military officials to get a better idea on exactly what information they would want him to collect.

But he never got the chance. Awwad was taken into custody on December 5, 2014, following another meeting with our undercover agent.

The USS *Gerald R. Ford* is still under construction, but when

completed, it will be the most advanced aircraft carrier in the world and the first in a new class of carriers. As a result of the joint FBI/NCIS efforts in this case, according to FBI Assistant Director Randall Coleman, "We prevented the loss of billions of dollars in research costs and the exposure of potential vulnerabilities to our newest generation of nuclear aircraft carrier."



# Solving Homicides

## FBI Forms Unique Partnership with Oakland Police Department



While searching for shell casings from a weapon that gang members used to kill an Oakland, California man in September 2015, FBI agents and Oakland Police Department detectives on the Homicide Task Force came across a marijuana grow operation in the warehouse where the victim was tortured before his murder.

On a peaceful, sunny morning in downtown Oakland, California, it is difficult to comprehend that the city across the bay from San Francisco is one of the most violent places in the country, with a murder occurring on average every three days. Inside the headquarters of the Oakland Police Department (OPD)—where homicide detectives and FBI agents were meeting—that reality is all too clear.

Seventeen months ago, the FBI dedicated 10 special agents to work alongside OPD detectives to investigate active homicides and more than 2,000 cold case murders that have taxed the department's historically understaffed homicide detective squad.

On this morning, agents and

detectives comprising the Homicide Task Force were discussing their most pressing investigations—almost all related to gangs and drugs—and how best to solve them. An OPD detective mentioned that a key witness in one of his cases had fled to Texas. FBI Special Agent Russ Nimmo, who leads the partnership effort, said agents in Texas could locate the witness there and arrange for an interview. “We can help with that,” he said.

It's just one example of how the FBI adds value and depth to OPD murder investigations. Not only does the Bureau assist by pursuing leads in other states but agents also conduct interviews, execute warrants, and, when necessary,

deploy specialized resources such as the SWAT team and the Evidence Response Team. The FBI can also collect and process critical firearms and DNA evidence, which may be too time-consuming and costly for OPD to take on alone. This real-time partnership gives local detectives a federal reach they did not have before—and in many cases that means violent offenders are also charged federally, which can result in stiffer sentences.

“This effort with OPD is designed to be sustained and ongoing,” Nimmo says. “It is important to solve every murder, whether it occurs in a wealthy neighborhood or a poor one. We are showing the community that the FBI is not just something you see on TV

or read about in newspapers. We are working to provide justice in communities where many people feel that nobody cares about them.”

“This is a valuable partnership,” added Lt. Roland Holmgren of the OPD Homicide Unit, “and we are seeing the fruits of our combined labors.”

Since the FBI-OPD effort officially began in June 2014, the task force has cleared twice as many murders as had been cleared in the past—a rate that increased from about 30 percent of homicides to 60 percent. And the task force is actively working its backlog of cold cases as well.

At OPD headquarters, a dedicated workspace for the task force was set aside and is being renovated using funds from both the Bureau and the city. Detectives and agents are expected to occupy their new, permanent quarters by the end of the year. The space will feature state-of-the-art equipment to aid in recording and reviewing subject interviews. Agents and detectives will also have access to FBI computer systems to aid their investigations.

Nimmo explained that the Bureau has many Safe Streets Task Forces around the country—consisting of local, state, and federal law enforcement partners—working to fight violent crime. The effort to embed FBI agents with OPD detectives represents an additional commitment. “And it sends a message,” he said: “If you kill someone in Oakland, we will catch you.”

One case the FBI worked jointly with OPD was a December 2013 drug-related murder in East Oakland that occurred in the parking lot of a large chain store a

# SEEKING INFORMATION

Murder Victim  
Oakland, California  
June 12, 2013

**AYA NAKANO**



## Cold Case

One of the more than 2,000 cold cases being worked by the FBI-OPD Homicide Task Force is the 2013 murder of Aya Nakano, who was gunned down an hour before his 23rd birthday after a traffic incident in Oakland. In September, the FBI announced a reward of up to \$25,000—in addition to a separate significant reward offered by Nakano’s family—for information leading to arrests and prosecutions.

The FBI and the Oakland Police Department are asking for the public’s help to identify the two individuals responsible for the murder, which occurred around 11 p.m. on June 12, 2013. The Bureau’s National Digital Billboard Initiative is also featuring the case as part of the public awareness campaign.

Nakano was driving home to Emeryville, California, when his car was involved in a minor accident with a silver, four-door sedan with tinted windows. The accident occurred at the intersection of Stanford Avenue and Market Street. After the accident, Nakano pulled over near the intersection, as did the sedan. Two suspects emerged from the sedan and fatally shot Nakano before driving away.

Anyone with information regarding the case should contact the Oakland Police Department at (510) 238-7950, their local FBI office, or the nearest American Embassy or Consulate.

*Note: This case may have been resolved since it was posted on our website. Please check [www.fbi.gov/wanted](http://www.fbi.gov/wanted) for up-to-date information.*

few days before Christmas. Damion Sleugh had arranged to buy five pounds of marijuana from 24-year-old Vincent Muzac. The deal went bad, and Sleugh shot Muzac, dumping his body in the parking lot before driving off.

With the FBI’s assistance, Sleugh was indicted federally in March 2014 on first-degree murder and other charges. A jury convicted him in July 2015, and last week the 28-year-old was sentenced to life in prison.

Nimmo has been working to help OPD detectives since 2010. “The Sleugh case, along with several others, made us realize the greater federal impact we could have if more agents were fully staffed with OPD detectives,” he said. “The results so far are not surprising, given the quality of agents and detectives assigned to the task force.” He added, “This level of partnership over this length of time is making a real difference, but there is still much more work to be done.”



# Newseum Goes “Inside Today’s FBI”

D.C. Museum Updates Popular Exhibit



This diagram shows the layout inside an SUV that was rigged to explode in New York's Times Square in 2010. The homemade bomb—which failed to explode—included this gas can, propane tank, pressure cooker, and these alarm clocks. The items are on display along with the vehicle.

Some of the FBI's biggest terrorism cases since 9/11—along with headline-grabbing espionage and cyber investigations—are featured in an exhibit that opens today in the nation's capital.

“Inside Today’s FBI: Fighting Crime in the Age of Terror” is an updated and expanded version of a popular, long-running exhibit at the Newseum, a museum devoted to news and journalism located a few blocks from FBI Headquarters in Washington, D.C.

A collaboration between the Bureau and the museum, “Inside Today’s FBI” will display evidence and artifacts never before seen by the public, including the blue Toyota Corolla abandoned by terrorist hijackers prior to the 9/11 attacks and the explosives-laden Nissan Pathfinder used in a failed attempt to bomb New York City’s Times Square in 2010. Parts of the homemade bomb—propane tanks, alarm clocks, and a pressure cooker—can be seen inside the vehicle. Also on display will

be items from the 2013 Boston Marathon bombing, including the handcuffs that restrained bomber Dzhokhar Tsarnaev.

More than 45 new artifacts have been added to the exhibit, which focuses on terrorism as well as recent espionage cases—such as the Russian spy investigation known as Operation Ghost Stories—and cyber cases, like Silk Road, in which the FBI dismantled a secret website that allowed individuals to buy and sell illegal drugs anonymously online.



"Inside Today's FBI: Fighting Crime in the Age of Terror" is an updated and expanded version of a popular, long-running FBI exhibit at the Newseum, a museum devoted to news and journalism located a few blocks from FBI Headquarters in Washington, D.C. The exhibit features some of the Bureau's biggest cases since 9/11.



"The FBI has had a long and successful partnership with the Newseum," said Mike Kortan, FBI assistant director of public affairs. "We are pleased that the expanded exhibit provides even more opportunity for people to learn about the FBI and our mission to protect the country."

The Newseum's original Bureau-related exhibit, "G-Men and Journalists: Top News Stories of the FBI's First Century," debuted in 2008 and was updated in 2011. In July 2015, the exhibit closed for

renovations and opens today in a larger space with more than 160 artifacts, most of which are on loan from the FBI.

The "G-Men and Journalists" exhibit was intended to be temporary but was so popular its run was extended indefinitely. Millions of people have seen it. Other items still on display from the original exhibit include the Unabomber's cabin; engine parts and landing gear from United Airlines Flight 175, which crashed into the World Trade Center South

Tower on 9/11; and the hiking boots worn by "shoe bomber" Richard Reid, who received al Qaeda training to blow up an American Airlines flight from Paris to Miami in December 2001. The belts passengers used to restrain Reid are also on display.

"After 9/11, the FBI's mission changed substantially to prevent another terrorism attack," Kortan said. "The Newseum exhibit captures a fascinating part of that transformation."

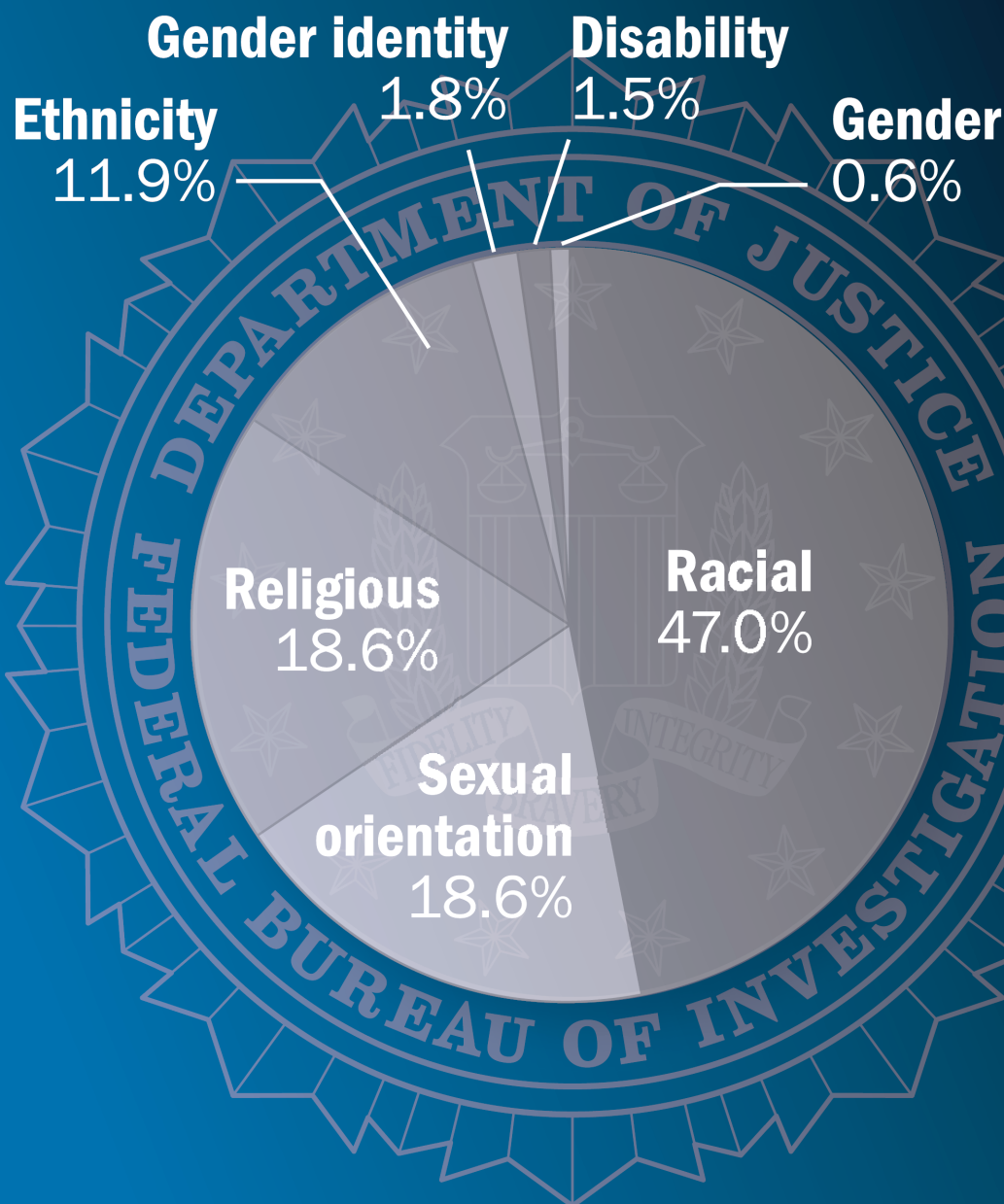


## Latest Hate Crime Statistics Available

Report Contains Info on Offenses, Victims, and Offenders

### Bias Breakdown

Analysis of the 5,462 single-bias incidents reported by law enforcement during 2014 revealed the following biases:



Of the 5,479 hate crime incidents reported in 2013, 5,462 were single-bias incidents, as detailed in the chart above.

According to the FBI's latest report, law enforcement agencies reported 5,479 hate crime incidents involving 6,418 offenses to our Uniform Crime Reporting (UCR) Program in 2014. And these crimes—which often have a devastating impact on the communities where they occur—left 6,727 victims in their wake.

The latest figures are down from 2013, when 5,928 criminal incidents involving 6,933 offenses were reported.

*Hate Crime Statistics, 2014* provides information about the offenses, victims, and offenders. Among some of the highlights:

- Of the 5,462 single-bias incidents reported in 2014, 47 percent were racially motivated. Other motivators included sexual orientation, religion, ethnicity, gender identity, disability, and gender. (See above chart.)
- Of the 6,418 reported hate crime offenses, 63.1 percent were crimes against persons and 36.1 percent were crimes against property. The remaining offenses were crimes against society, like illegal drug activity or prostitution.
- The majority of the 4,048 reported crimes against persons involved intimidation (43.1 percent) and simple assault (37.4 percent).
- Most of the 2,317 hate crimes against property were acts of destruction, damage, and vandalism (73.1 percent).
- Individuals were overwhelmingly the most common victim

of a single-bias hate crime, accounting for 82.4 percent of the reported 6,418 offenses. The remaining victim types were businesses, financial institutions, religious organizations, government, and society or the public.

- Also during 2014, law enforcement agencies reported 5,192 known offenders in 5,479 bias-motivated incidents. (In the UCR Program, “known offender” does not imply that the suspect’s identity is known, only that some aspect of the suspect was identified by a victim or witness—such as race, ethnicity, or age.)

*In addition to releasing annual Hate Crime Statistics reports, which give the nation a clearer picture of the overall crime problem, the FBI also investigates incidents of hate crimes—as a matter of fact, it’s the number one priority within our civil rights program.*

And while 15,494 law enforcement agencies contributed to UCR’s *Hate Crime Statistics* report in 2014, only 1,666 agencies reported hate crimes within their jurisdiction (the remaining agencies reported zero hate crimes).

To enhance the accuracy of hate crime reporting, representatives from the UCR Program

participated in five hate crime training sessions provided jointly by the Department of Justice (DOJ) and the FBI. Since April 2015, DOJ and the FBI provided the training sessions to law enforcement agencies and community groups in several different areas of the county. UCR personnel also worked with states to ensure proper data submission and met with police agencies to provide training and discuss crime reporting issues.

In addition to releasing annual *Hate Crime Statistics* reports, which give the nation a clearer picture of the overall crime problem, the FBI also investigates incidents of hate crimes—as a matter of fact, it’s the number one priority within our civil rights program. We investigate hate crimes that fall under federal jurisdiction, assist state and local authorities during their own investigations, and in some cases—with the DOJ’s Civil Rights Division—monitor developing situations to determine if federal action is appropriate.

The 2016 release of the *Hate Crimes Statistics* report, which will contain 2015 data, will feature even more information—expanded bias types in the religion category and the added bias type of anti-Arab under the race/ethnicity/ancestry category. The collection of both types of data began in January 2015.



# International Operations

## Building Partnerships in the Americas

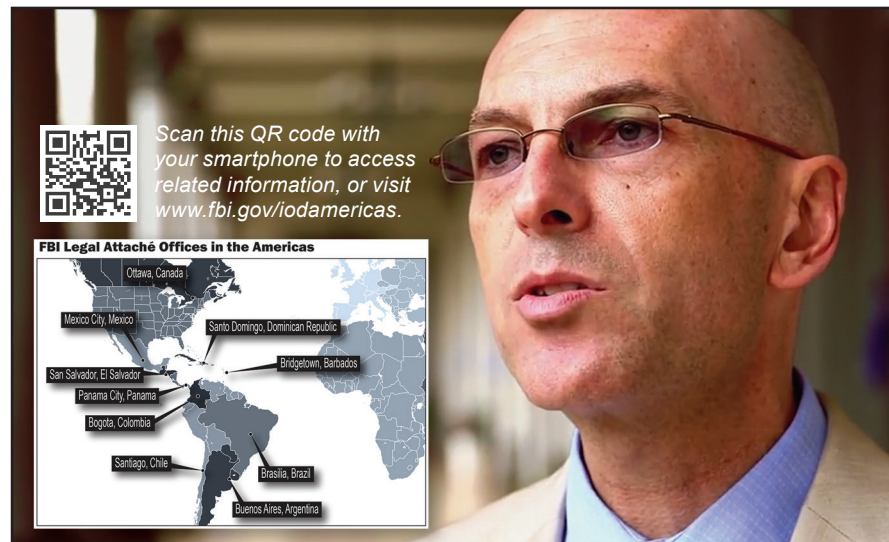
Members of the FBI's International Operations Division who work in North, Central, and South America carry out their mission in some of the most violent countries in the world and face criminal threats—such as drug cartels and transnational gangs—that spill across borders and threaten the safety of Americans at home and abroad.

Some of the most potent weapons against these threats are strong and lasting partnerships—not only among U.S. federal agencies but also with international allies.

“In the Americas, the drug dealers, gangs, and human traffickers do not recognize borders,” explained Special Agent David Brassanini, chief of the Americas Unit in the FBI's International Operations Division. “That is why partnerships with our host countries and fellow federal agencies are so important. We can only fight these violent criminals through strong alliances,” he said, adding that while many Americans think of the FBI as primarily a domestic law enforcement organization, “our presence abroad is strong, as it must be to protect the homeland.”

At a recent conference at the United States Southern Command (SOUTHCOM) military headquarters in Florida were the FBI's legal attachés—or legats—who cover the Americas: the Bureau has offices in Argentina, Barbados, Brazil, Canada, Chile, Colombia, Dominican Republic, El Salvador, Mexico, and Panama.

Holding the conference at a Department of Defense (DOD) facility was fitting, because the military is a key FBI partner in the Americas. Both organizations have personnel cross-assigned in liaison



David Brassanini, chief of the Americas Unit, discusses the FBI's operational role working with partners in countries stretching from Canada to Argentina.

roles so that intelligence can be shared seamlessly and operations can be carried out jointly.

“The Bureau and the DOD tend to look at threats the same way and seek to disrupt and dismantle them by working together,” said an FBI agent stationed at SOUTHCOM, one of nine combatant commands within the DOD.

“SOUTHCOM's most important mission is to protect the southern approaches to the United States,” said Gen. John F. Kelly, SOUTHCOM commander.

“We do not and cannot do this mission alone. We work side by side with the FBI and other law enforcement professionals to defend the U.S. homeland against transnational criminal networks, illicit trafficking, and the threat of terrorism.”

Participants at the conference—including other federal law enforcement agencies—were briefed on recent investigations and a variety of criminal trends relating to terrorism, cyber intrusions, espionage, and more. The overwhelming crime issues in the Americas stem from transnational

gangs and criminal organizations that traffic in drugs and people. These groups routinely murder, extort, and commit other crimes in the region, and those crimes have an impact inside the United States.

“The gang violence in Central America, particularly in El Salvador, has really taken off lately,” Brassanini said, “and we have seen an influx of that violence to the U.S. In many cases, Central American gang leaders are ordering crimes and murders committed in the U.S.”

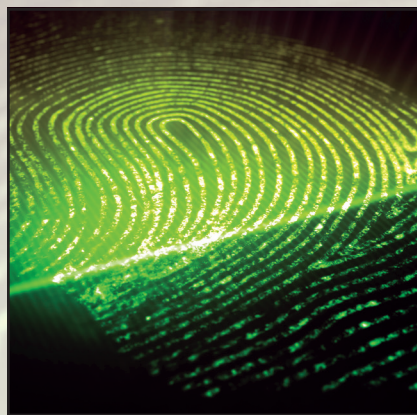
Being vigilant about crime in the Americas is important because the countries there are U.S. “touch points,” Brassanini said. “The Americas touch us by land and by sea,” he explained. “That is why we work so closely with our partners to share intelligence, provide training, and bring these criminals to justice.”

The partnerships are working. “Our accomplishments are significant,” Brassanini said. “Almost on a daily basis we are able to identify and track down violent criminals, and that makes all our countries safer.”



# 2015 Biometric Identification Award

## Virginia Police Investigator Honored for Role in Identifying Violent Perpetrator



The 2015 recipient of the FBI's Biometric Identification Award (formerly known as the Latent Hit of the Year Award) is a member of Virginia's Norfolk Police Department (NPD) who played a key role in the identification of a dangerous serial offender. Congratulations to Melvin Grover III, an investigator with the forensic section of the NPD's detective division.

This Criminal Justice Information Services (CJIS) Division award is traditionally given to a latent print examiner or law enforcement officer who solves a major violent crime using the FBI's Integrated Automated Fingerprint Identification System, or IAFIS. But IAFIS—our longstanding fingerprint repository—was replaced last year by the Next Generation Identification (NGI) system, developed to expand the Bureau's biometric identification capabilities and services, and future awards will involve the use of the NGI system.

The case Grover eventually became involved with started in August 2008, when the NPD received an emergency call from a private residence and responding officers found a female tied up in a locked bathroom. The victim, a U.S. Navy officer, said that she had been

sleeping and was awakened by an unknown male brandishing a knife. The man raped her, bound her legs with the cord of an iron, and stole items from the home before fleeing.

Investigator Wade Stalker of the NPD processed evidence from the scene, including latent fingerprints from the iron and a door. Grover searched all the latent print evidence against Virginia's Automated Fingerprint Identification System but got no results.

In September 2008, the victim and her daughter returned home one day and were confronted by the same attacker. He tied them both up with duct tape and raped the daughter before fleeing the scene. Once again, investigators collected evidence, including latent fingerprints and DNA. The prints were compared against Virginia's system, which didn't produce any known suspects but did confirm that the same individual committed both crimes. Investigators also searched the collected DNA evidence against the FBI's Combined DNA Index System, or CODIS, with no results. The case remained unsolved.

In the spring of 2010, a female service member stationed in Kuwait was attacked while in a shower. An unknown male with a shirt covering his face went after the victim with a box cutter, but she fought back and the suspect ran off. Personnel from the U.S. Army Criminal Investigation Command collected blood samples from the shower and from a secondary crime scene where a blood-stained shirt was recovered from the trash. DNA isolated from the blood samples was searched against CODIS and positively linked to the two 2008

attacks in Norfolk. But the actual identity of the attacker remained unknown.

In January 2012, representatives from the Naval Criminal Investigative Service (NCIS) met with Investigator Grover of the NPD to discuss the cases, and latent fingerprint evidence from both crimes scenes was searched against the Bureau's IAFIS, with negative results. Later on, NCIS contacted the CJIS Division's Latent and Forensic Support Unit (LFSU) to coordinate investigative efforts with the NPD. LFSU personnel conducted an internal search of the latent fingerprints collected against the Bureau's repository of civil prints—at that time, IAFIS—and forwarded possible candidates to Investigator Grover. Grover was able to determine that the prints matched those of Amin Garcia, who had served in a Navy reserve unit and whose time in duty stations in Norfolk and Kuwait coincided with the attacks.

NCIS was then able to obtain a sample of Garcia's DNA, which matched the DNA evidence left at the Norfolk and Kuwait crime scenes. In January 2014, Garcia was arrested in New York City and extradited to Virginia.

Garcia was convicted after a three-day trial for his crimes in Norfolk, and in December 2014, he was sentenced to life in prison plus 120 years. For the Kuwait attack, he was indicted in October 2014 by a federal grand jury, and that case is still pending.

Thanks to the skills and dedication of a Norfolk Police Department investigator—and technology—a violent predator was identified and taken off the streets.



# Agents of Asian Ancestry

'Historical Marker' Celebrates 50 Years of Service



When William Wang joined the FBI as a special agent in 1966, the number of known agents of Asian ancestry could be counted on one hand. There was no official tally, Wang said, because Director J. Edgar Hoover didn't find it necessary to keep count.

"Under Mr. Hoover, you are either a special agent or not a special agent," said Wang, who was born in China, immigrated to the United States in 1956, and became the Bureau's fifth known agent of Asian ancestry. "As far as he was concerned, we're all special agents—period."

Over the years, Wang took it upon himself to keep track of the number, and he reached out personally to new agents of Asian descent as they came through training at the FBI Academy in Quantico, Virginia. "It was important to me to just let them know that I'm here," he said.

The role of agents of Asian ancestry over the past 50 years—

since Edwin Yee and Calvin Shishido were sworn in as agents in 1965—was a centerpiece of this year's annual national conference of the Society of Former Special Agents of the FBI. Retired Special Agent Ellen Glasser, who was president of the society during the September gathering in Reno, Nevada, said it was a fitting time to honor them for the "special value and needed diversity" they brought to the FBI's ranks.

"We decided this was an opportunity to do something really important and to create a historical marker for their 50 years of service," Glasser said, speaking to hundreds of former agents, but specifically addressing the cadre of Asian former agents in attendance. "By celebrating your achievements and your loyalty, we here in the FBI family want to publicly say thank you and job well done."

In conversations, many recalled being recruited into the Bureau specifically because of their

Left: Fred Wong, seen here taking the FBI oath, became a special agent in 1982. He played a key role in the arrest of a Top Ten fugitive in 1984, and served as head of FBI offices in Belgium and Indonesia before retiring in 2007.

backgrounds, both professional and ethnic.

Kingman Wong, who served from 1988 to 2012, said the San Francisco Field Office was looking for agents with Chinese language skills when he was recruited. He landed on an Asian organized crime squad there, which propelled him to other undercover assignments in Hong Kong and Thailand.

"In terms of infiltrating these groups, you have to know the culture, you have to know the language," he said. "It would be very difficult if the Bureau sent in a Caucasian agent."

Chris Loo also worked in the San Francisco office, from 1978 to 1999. He remembered his boss assigning him to applicant recruitment, specifically to reach out into the Asian community. He did that successfully for two years—hiring a number of future legal attachés to run our overseas offices—before returning to an organized crime squad, where he helped launch the office's Asian organized crime program.

"Your ethnicity certainly helps open doors in the community," said Loo, recalling an interview with a potential witness who was Chinese. "He was very hesitant to speak to me, and his sponsor said, 'Don't be afraid to speak to Mr. Loo. He's with the FBI and he's Chinese.' I found the ethnicity a plus in helping to get the foot in the door."

The former agents also encountered some strains of



**Left: Retired agents of Asian ancestry reflect on their experiences and perspectives in videos on our website.**

discrimination but generally brushed it off and rose above it. JoAnn Sakato, who served from 1978 to 2002 and was the first Asian woman agent in the FBI, chalked up any racist or sexist slights to ignorance.

“As a Japanese female, I think some of the agents expected a geisha,” she said. “Well, that’s not what they got when they hired me. A funny story is that in the Los Angeles Field Office they would call me Dragon Lady. I suppose in some contexts it could be a derogatory term. I decided to adopt that as my moniker and made it my own. I guess I established certain reputation for taking no prisoners. I adopted that, and that was my persona.”

Today there are nearly 600 active special agents of Asian ancestry, a figure roundly regarded as too low. Director Comey frequently cites the FBI’s diversity statistics in public remarks about how the FBI needs to better reflect the people it serves.

“Diversity is about doing the right thing, but also about effectiveness,” Comey said at the National Organization of Black Law Enforcement Executives annual meeting last March. “It’s about being good at what we do. We are simply less effective when we are less diverse.”

The earliest Asian agents largely dismiss the descriptive modifier in their title—much as the first women agents did in 1972. Like his colleagues, Joe Louie, the third known Asian to be hired as an agent in 1966, just wanted to be called an agent—period. “I don’t think they really cared if you were black, white, or purple,” he said. “If you were selected for being an agent, that was a prime job.”

Frederick Wong’s career, from 1982 to 2007, may best illustrate the point. He was one of Chris Loo’s hires who went on to become a legal attaché, not once but twice. His first overseas office was in Belgium. “I remember some of my colleagues in Belgium, the Netherlands, and Luxembourg,

they were quite surprised, but pleasantly surprised that ‘you aren’t all white agents,’” he said. “It was a big plus. It helped me open doors.”

## Changing Perceptions

In his 30 years as an FBI agent, from 1982 to 2012, Weysan Dun worked his way up the management ladder. He was a special agent in charge (SAC) of three field offices and saw firsthand, repeatedly, how important it is to reflect the people you serve. In an interview, he described the evolving perception of law enforcement in the Asian community and why it’s important to have senior agents of Asian ethnicity in the Bureau.



“Some of the ethnic communities with which I had to deal, I think were partly disarmed by the fact that they never expected to see an Asian

guy as the head of the FBI office.

“When I was an SAC in Newark, the local Asian community there actually was so enthralled that there was an FBI executive of Asian ethnicity because they never even dreamed that was a possibility...they actually did an article for me in a Chinese language periodical (above). They were just amazed that there was an Asian executive in the FBI. Frankly, as a result of that, it caused them to say, ‘We really need to be a little more open and welcoming when we do run across the FBI.’ ”



Scan this QR code with your smartphone to access related information, or visit [www.fbi.gov/asianagents50](http://www.fbi.gov/asianagents50).



# Want to Obtain FBI Records a Little Quicker?

## Try New eFOIA System



*Note: eFOIA open beta testing ended December 21, 2015. Submissions will be accepted after system updates are made.*

The FBI recently began open beta testing of eFOIA, a system that puts Freedom of Information Act (FOIA) requests into a medium more familiar to an ever-increasing segment of the population. This new system allows the public to make online FOIA requests for FBI records and receive the results from a website where they have immediate access to view and download the released information.

Previously, FOIA requests have only been made through regular mail, fax, or e-mail, and all responsive material was sent to the requester through regular mail either in paper or disc format. "The eFOIA system," says David Hardy, chief of the FBI's Record/Information Dissemination Section, "is for a new generation that's not paper-based." Hardy also notes that the new process should increase FBI efficiency and decrease administrative costs.

The eFOIA system continues in an open beta format to optimize the process for requesters. The Bureau encourages requesters to try eFOIA and to e-mail [foipaquestions@ic.fbi.gov](mailto:foipaquestions@ic.fbi.gov) with any questions or difficulties encountered while

using it. In several months, the FBI plans to move eFOIA into full production mode.

Here's what you need to know to assist the FBI in testing the eFOIA system:

- You are limited to one request per day.
- So the FBI is confident in the identity of the requester, you will need to provide a valid e-mail address and a government-issued form of identification in one of the following formats: .pdf, .doc, .png, .gif, .jpg, or .jpeg.
- Your requests are limited to information about organizations, events, or deceased individuals.
- If you are requesting information on a deceased individual, you will need to upload proof of death unless the deceased individual is more than 100 years old. Acceptable proof of death includes obituaries, death certificates, recognized sources that can be documented, written media, *Who's Who in America*, an FBI file that indicates a person is deceased, or a Social Security Death Index page.
- The maximum combined size of all attachments in a request is 30 megabytes.

- Regulatory FOIA fee schedules remain in effect for eFOIA requests.
- Audio and video files, because of their large size, must be sent to requesters through standard mail.

A quick note: If you want to make what's called a "first party" request asking for information about yourself or another living person—which falls under the U.S. Privacy Act (PA)—you will need to mail, fax, or e-mail the U.S. Department of Justice's Certification of Identity Form DOJ-361, plus any additional information that may help in locating the records you're looking for, to the FBI.

Submissions to the FBI's overall FOIA/PA program continue to trend upward, according to Hardy. "Requests have increased over the past decade by as much as a third," he said. "Over the past year, we've received approximately 18,500 requests and, thanks to a skilled workforce and increasing automation, we were able to review for release 1.1 million pages."

And while many of the requests that come in are from the media, authors, academia, organizations, and the like, Hardy noted that 40 percent of FOIA/PA requests come from individuals looking for records on themselves.

The original purpose of the decades-old Freedom of Information Act and the Privacy Act was to promote openness in government. "Our belief in the concept of government transparency and the public's right to access certain records held by government agencies is what continues to drive us to this day," said Hardy, "and eFOIA represents another step by the FBI to enhance that access."

# FBI Celebrates 75th Anniversary of Legat in Mexico City

## Milestone Marks Longstanding Crime-Fighting Alliance

The FBI's office in Mexico City—the Bureau's largest and oldest overseas post—marked its 75th anniversary yesterday, commemorating the longstanding alliance between the U.S. and Mexico in the fight against crime.

The FBI and Mexican authorities have been working together since the early 20th century, with the Bureau's legal attaché office in Mexico City officially opening in 1940. The FBI maintains more than 60 legal attaché offices—or legats—around the world, where Bureau personnel work closely with host countries to share information and to coordinate investigations that help safeguard American citizens and protect U.S. interests.

Applauding the 75-year milestone in a recorded video shown during yesterday's ceremony in Mexico City, FBI Director James Comey called it “a testament to the strength of our partnership.” He added that today's criminals and terrorists “no longer recognize borders or boundaries. We face truly global threats, and we must confront these challenges as a global law enforcement community.”

The U.S. and Mexico “share a common vision toward tackling crime,” said Special Agent Eric Drickersen, who heads the FBI's Mexico City Legat. In the 1940s, during World War II, the Bureau's efforts in Mexico and South America largely involved locating Nazis who had infiltrated North America, but even then, agents and Mexican authorities collaborated on a variety of criminal matters.

“The FBI was very forward-thinking in those days, when evidence of the impact of international crime first surfaced,”



During a ceremony in Mexico City on December 3, 2015, Legal Attaché Eric Drickersen, Criminal Investigative Division Assistant Director Joseph Campbell, and International Operations Division Deputy Assistant Director Robert Johnson (left to right) marked the 75th anniversary of the Bureau's official presence in Mexico.

Drickersen said. “The Bureau recognized early on the necessity to collaborate with international partners. Mexico was one of our natural initial partners because we share a border and because crimes impacted both nations.”

Over the years, those crimes have evolved. Today, multi-national criminal organizations traffic drugs and people, and violent gangs carry out kidnappings and extortions on both sides of the border. “Without collaboration between the U.S. and Mexico,” Drickersen explained, “it would be virtually impossible to deal with the level of crime we now face.”

The crime-fighting coalition between the two countries has resulted in many successes, perhaps none more apparent than the FBI's fugitive program. With the assistance of Mexican law enforcement, a total of 18 of the FBI's Ten Most Wanted Fugitives have been captured in Mexico and returned to the U.S.—more than from anywhere else in the world. The most recent example is Top Ten fugitive Jose Manuel Garcia Guevara, who was apprehended in

Mexico last year and returned to Louisiana to face rape and murder charges.

Another important aspect of the U.S.-Mexican law enforcement alliance is training. From the outset, police officers from both countries have trained together. The FBI's internationally respected National Academy—a professional development course for U.S. and overseas law enforcement personnel—has counted nearly 50 Mexican officers among its graduates since the 1940s.

“The Bureau continues to provide training to our Mexican law enforcement partners on topics ranging from managing crime scenes and interviewing subjects to complex cyber investigations,” said Drickersen.

“Today's anniversary recognizes the importance of all aspects of the FBI's partnership with Mexico,” he added. “For three-quarters of a century, we have built a coalition that has grown and continues to grow. The FBI is very proud of that.”



# Model Partnership

## New York Joint Terrorism Task Force Celebrates 35 Years

It was a spring afternoon in 1980 when a special agent from the FBI's New York Field Office and a New York City Police Department official met for lunch to discuss how to combine their expertise to track down terrorist organizations responsible for a wave of violent attacks in the city.

That meeting led to the pooling of both agencies' resources into a group that became known as the Joint Terrorism Task Force, or JTTF. And last week in New York, the FBI and NYPD celebrated the work the JTTF has been doing ever since.

In a December 1 ceremony at the FBI's New York Field Office marking the JTTF's 35th anniversary, FBI Director James Comey described the New York JTTF as the "granddaddy of them all" in a recorded video message shown at the event. "This was the one that started the model, that helped bring the NYPD and the FBI together in ways that people never thought possible," said Comey.

The JTTF concept has expanded from its roots in New York to 104 cities nationwide. Now approximately 4,000 members from more than 500 state and local agencies and 55 federal agencies work together to investigate and prevent domestic and international terrorism. Made up of highly trained investigators, analysts, SWAT team experts, and other specialists, these groups of law enforcement and intelligence personnel are the front line in the fight against terrorism.

Since its inception in 1980, the New York JTTF has been instrumental in this fight. It has aggressively investigated criminal



Members of the FBI New York's JTTF in the Joint Operations Center immediately following a May 2010 attempted bombing in Times Square.

activity, including a 2007 plot to bomb John F. Kennedy Airport, a 2009 plot to attack New York's subway system, and a 2010 attempted bombing in Times Square. The New York JTTF also took part in investigating international events like the U.S. Embassy bombings in East Africa in 1998 and the 2000 terrorist attack on the USS Cole in Yemen.

Lethal attacks like the 1993 bombing of the World Trade Center and the tragic events of 9/11 created a need for JTTFs nationwide to increase their investigative resources and collaborative efforts to combat terrorism on a national and international scale. The New York JTTF has provided an effective framework for other task forces to follow.

"Here in New York, we have the largest JTTF in the country and we could not expect to thrive without the support of our local, state, and federal agencies," said FBI New York Assistant Director in Charge Diego Rodriguez at last week's ceremony. "It's through

partnerships like this that we continue to explore a multifaceted approach to fighting crime."

Today, these interagency teams of experts are working across the country to prevent terrorism. JTTFs are responding to leads, gathering evidence, and sharing intelligence amongst numerous local and state law enforcement agencies as well as federal organizations such as the Department of Homeland Security, the U.S. military, Immigration and Customs Enforcement, and the Transportation Security Administration.

"The JTTF brings together the resources that have made us successful in fighting terrorism," said Director Comey. "The threat that we face today is one that the JTTFs were made for. It's a threat that's dispersed and very hard to see. We need the help with resources and surveillance. We especially need the eyes and ears of our local partners. Our being knit together through the JTTF is the strength of our response."

# Human Trafficking

## Prison Time for Men Who Attempted to Buy Sex Slaves

During the course of an international human trafficking investigation, FBI agents uncovered disturbing information: American men were making what appeared to be serious inquiries about buying kidnapped women from Asia to serve as sex and domestic slaves.

“This case opened people’s eyes to a much darker side of human trafficking than we were previously aware of,” said Special Agent Ryan Blay, who worked the investigation from the FBI’s Phoenix Division.

The case started in 2012, when agents were alerted to an advertisement from Malaysia on the now-defunct bondage website collarme.com, purporting to sell kidnapped Asian women “who are naturally very obedient.”

The online solicitation turned out to be a money-making scam, Blay said, but the response from potential customers in the U.S.—nearly 200 inquiries during a two-month period—was “alarming.” After the fraudulent advertisement was removed from the website and the FBI referred the matter to Malaysian authorities, Blay and his team devised an undercover operation targeting the same clientele.

“The idea was to be proactive, to identify these individuals and stop them before they could actually victimize anyone,” he said. The FBI created an undercover platform advertising kidnapped women for sale as sexual and domestic slaves.

“Almost immediately there were responses,” Blay said. “We weren’t interested in individuals who were just pursuing some sort of fantasy,” he explained. “The only people we wanted were those who were serious about buying kidnapped women.”



**Evidence seized in the human trafficking case, such as these restraints, revealed that the subjects were fully prepared to buy kidnapped women and hold them against their will.**

The undercover operative posing as the seller “actually tried to talk people out of it,” Blay said. “He stressed that these women would be taken against their will and the transaction would be illegal in every possible way.”

More than 100 people responded, and most dropped out quickly. But four individuals were anxious to proceed—and willing to pay thousands of dollars for a sex slave. “All of them said this was something they had wanted to do for a long time,” Blay said.

The undercover operative told the four buyers he was connected to a human trafficking group that would identify foreign females in the U.S. on temporary visas, kidnap them, and sell them into a life of slavery. The operative also said his organization held a biannual auction, where the women would be sold to the highest bidders.

The four individuals—two from Arizona, one from Montana, and one from California—were in their 50s and 60s. One was an engineer with a Top Secret government clearance. Another was a financial analyst. The Montana man was going to pay \$10,000 for two women. When he flew to Phoenix

in May 2014 to make the purchase, he was carrying u-bolts to bind the women’s wrists and gags to keep them quiet. He planned to transport them back to Montana in a recreational vehicle. The man told the undercover operative he had a fully functional dungeon in the basement of his home.

“When we eventually conducted searches,” Blay said, “all the subjects had basically manufactured rooms in their homes to be prison cells. There were bars on windows, obscured glass, and insulation so no one could see or hear the women from the outside. One guy bolted chains in the floorboards of a room.”

The four men were indicted on human trafficking charges between December 2013 and May 2014. They all pled guilty, and in September 2015, an Arizona federal judge sentenced them to prison terms ranging from seven to nine years.

“We are extremely pleased that we were able to intervene before any of these individuals was able to hurt anyone,” Blay said. “We didn’t want to wait until there were actual victims.”



# 2014 Expanded Crime Statistics Released

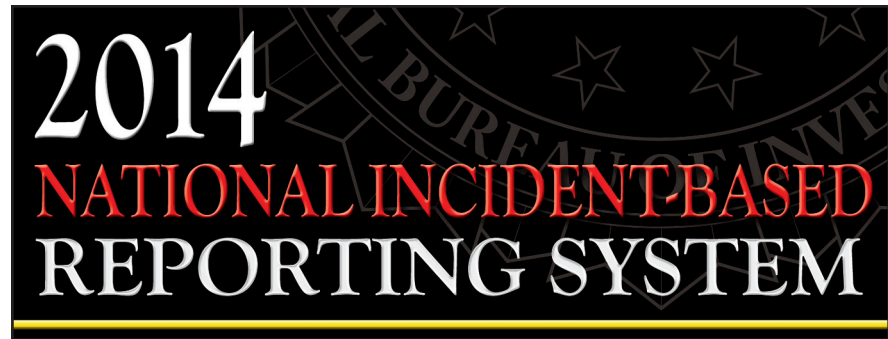
## National Incident-Based Reporting System Includes More Detailed Data

Today, the FBI's Uniform Crime Reporting (UCR) Program released details on more than 5.4 million criminal offenses reported by law enforcement through the National Incident-Based Reporting System (NIBRS) during 2014. According to NIBRS, 2014, 6,520 law enforcement agencies—charged with protecting more than 93 million U.S. inhabitants—reported 4,759,438 incidents involving 5,489,485 offenses, 5,790,423 victims, and 4,414,016 known offenders.

Among the report's highlights:

- Of the offenses reported during 2014, 63.6 percent involved crimes against property, 23 percent involved crimes against persons, and 13.4 percent included crimes against society (so-called “victimless” crimes like gambling).
- There were 4,414,016 known offenders, meaning that at least one characteristic of the suspect—such as age, sex, or race—was known. Of these offenders, nearly a third (32.3 percent) were between 16 and 25 years of age, the majority (63.9 percent) were male, and more than half (57.1 percent) were white.
- Concerning the relationship of victims to known offenders, 52.7 percent of the 1,273,602 victims knew the individual perpetrating the crime but were not related to them. Nearly a quarter of the victims (24.8 percent) were related to their offenders.

In addition to the standard data tables, this year's NIBRS report includes a brand new feature: an interactive map that allows users to click on a state, view map pins for each agency, select a pin, and get



a dropdown listing of that agency's offense data for 2014.

NIBRS, 2014 also includes a monograph on sex offenses previously reported by law enforcement that demonstrates the benefit of NIBRS data in allowing a more granular examination of a topic.

Unlike data reported through UCR's traditional Summary Reporting System (an aggregate monthly tally of crimes) and published annually in *Crime in the United States*, NIBRS data goes much deeper because of its ability to provide circumstances and context for crimes. It includes all offenses within a single incident as well as additional aspects about each event, like location, time of day, relationship between victim and offender, and whether the incident was cleared. NIBRS also includes data on 23 offense categories made up of 49 offenses, as opposed to the Summary Reporting System's 10 Part I offenses. Ultimately, NIBRS will improve the detail and overall quality of crime data, which will help law enforcement and communities around the country use resources more strategically and effectively.

However, only about a third of all U.S. law enforcement agencies currently participate in NIBRS. Transitioning to the new system

can be somewhat costly, and—because of the greater level of reporting specificity in NIBRS—it can initially appear that an agency has higher levels of crime after switching to NIBRS.

But because NIBRS can provide more useful statistics that will promote constructive discussion, measured planning, and informed policing, FBI Director James Comey has made across-the-board implementation of NIBRS one of his top priorities. At a recent International Association of Chiefs of Police (IACP) conference in Chicago—a video excerpt of his remarks is included in this latest NIBRS report—he talked about the importance of this program: “We face a data shortage on the violent crime front. We can't tell you on a national level how many shootings there were in any particular city last weekend,” Comey said. “How can we address a rise in violent crime without good information? And without information, every single conversation in this country about policing and reform and justice is uninformed, and that is a very bad place to be.”

And influential organizations like the IACP, the National Sheriffs' Association, the Major City Chiefs Association, and the Major County Sheriffs' Association agree—all have pledged their support for NIBRS.

# New Top Ten Fugitive

## Help Us Find a Violent Criminal

Myloh Jaqory Mason—wanted for a series of violent crimes, including attempted murder—has been named to the Ten Most Wanted Fugitives list.

A reward of up to \$100,000 is being offered for information leading directly to the arrest of the 25-year-old fugitive, who is being sought on federal and state charges for his alleged involvement in recent violent bank robberies and two separate shootings in Lakewood, Colorado.

“Myloh Mason is a very violent felon. It’s important for the safety of the community that we apprehend him as soon as possible,” said Special Agent Russ Humphrey, fugitive coordinator for the FBI Denver Field Office’s Rocky Mountain Safe Streets Task Force.

Along with two accomplices—who are in custody—Mason is believed to have robbed at least two Lakewood banks within the last four months, and his tactics have become more aggressive. The first robbery took place on September 30, 2015. Mason and two others wearing costumes allegedly shoved guns in the faces of bank employees and said the tellers would be killed unless they opened the bank vault.

The crew struck again in November. Mason and two others allegedly wore green and white skeleton masks when they staged a takeover robbery, shoving guns in the faces of tellers to gain access to the vault. During that robbery, Mason—a convicted felon—was wearing a ballistic vest. Pursued by police after fleeing the bank, Mason and his partners shot two innocent citizens during a home invasion and a carjacking.

“The robbers clearly seemed desperate,” Humphrey said. “It



was lucky that the two injured civilians, one of whom was shot four times, weren’t killed.” He added that the scenes played out near schools—which were locked down for hours—and a community recreation center frequented by parents with young children.

“We do not accept this kind of ruthless violence in our communities,” Humphrey said. “Adding Mason to the Ten Most Wanted Fugitives list is an indication of how serious we are about apprehending him.”

***Mason is the 505th person to be placed on the FBI’s Ten Most Wanted Fugitives list, which was established in 1950.***

Mason is 6-foot-2 and weighs approximately 155 pounds. He has black hair, brown eyes, and tattoos on his chest, both arms, and hands. He has ties to Colorado, Florida, and Nevada. Investigators say that he uses a variety of aliases and caution that he should be considered armed and extremely dangerous.

“Mason and his gang have committed some of the most

violent bank robberies we’ve seen in Colorado,” said Thomas Ravenelle, special agent in charge of the FBI’s Denver Division. “We believe he’s not going to stop and is a real danger to the community.” Ravenelle urged the public to help the FBI catch Mason and noted the substantial reward for cooperation.

If you have any information concerning the whereabouts of Mason, please call the FBI at 1-800-CALL-FBI (225-5324), or contact your nearest FBI office, law enforcement agency, or U.S. Embassy or Consulate. You can also submit a tip online.

Mason is the 505th person to be placed on the FBI’s Ten Most Wanted Fugitives list, which was established in 1950. Since then, 473 fugitives have been apprehended or located, 156 of them as a result of citizen cooperation.

*Note: Myloh Jaqory Mason was taken into custody without incident on January 15, 2016.*



# Violent Carjackers Sentenced

## Law Enforcement Partnerships Have an Impact

From late December 2012 to mid-January 2013, a series of violent carjackings in and around the Atlanta metro area shook the region and caused a significant violent crime spike. But a partnership between the FBI and law enforcement authorities in Cobb, Fulton, Gwinnett, and DeKalb Counties resulted in the dismantlement of the dangerous gang of criminals responsible.

And seven of those criminals were recently sentenced to federal prison terms, including the leaders of the so-called Bandits street gang, Ladarious Gibbs and Derek C. Turner.

The defendants were charged in connection with at least seven carjackings. During these crimes, the victims were typically accosted as they were entering or exiting their vehicles. Using a particularly frightening modus operandi, one gang member would approach from the victim's right side while the other would approach from the left, both pointing firearms and demanding the car. The carjackers were brazen—many of the incidents took place in daylight and at locations where the victims—young, middle-aged, and elderly—were going about their daily lives, such as libraries, shopping malls, gyms, bars, etc.

Accounts from the victims were harrowing. For example, a young woman who was eight months pregnant ended up going into pre-term labor and had to be hospitalized. In another case, shortly after one carjacking incident, the criminals raced onto a nearby interstate and crashed the stolen vehicle into a median—but when a couple of good Samaritans stopped to help, they themselves were carjacked. And during



Shown above is one of the vehicles stolen by members of the Atlanta-area “Bandits” street gang during a series of violent carjackings over a three-week period beginning in late December 2012.

another carjacking that took place in front of a department store, a passerby—who happened to be a store employee—was shot in the leg and suffered serious, long-term medical issues.

Eventually, local law enforcement agencies were able to link several of the vehicles that the suspects traveled in as well as bullet shell casings found at the crime scenes. Some of the suspects also bragged about their exploits in a video posted on a social media website. And one individual took picture of himself with a victim's cell phone—unbeknownst to him, the photos were saved to the victim's cloud computing account.

In February 2013, six individuals were charged at the state level—of those, five were taken into custody by the Atlanta Police Department. But because of the multi-jurisdictional nature of the crimes, the fact that some of the suspects were repeat offenders, and because the federal carjacking statutes provided for harsher penalties, local authorities began looking into the possibility of federal charges and asked for the assistance of the Atlanta FBI Office.

Bureau investigators—working hand in hand with the U.S.

Attorney's Office for the Northern District of Georgia, the Cobb County and Atlanta Police Departments, and local prosecutors—conducted additional interviews, sent DNA evidence and latent fingerprint evidence to the FBI Laboratory, and analyzed suspects' phones. An additional suspect was identified, and there was enough evidence gathered against Bandit gang members to convince a federal grand jury to begin handing down indictments in July 2013. A final superseding indictment was filed in May 2014.

After the sentencing of Gibbs, Turner, and three other co-conspirators, FBI Atlanta Special Agent in Charge J. Britt Johnson said that cases like this one require “the combined efforts and resources of law enforcement working together and across jurisdictional boundaries to get these violent offenders off our streets and into prison.”

This same sentiment is echoed in communities around the country wherever FBI investigators and state and local law enforcement personnel join together to target violent criminals who threaten public safety.

# Drug Trafficking

## Aryan Brotherhood Methamphetamine Operation Dismantled

When a federal judge recently sentenced the last two of 34 Aryan Brotherhood of Texas gang members to prison for their roles in a methamphetamine drug distribution network, it marked the end of the gang's foothold in Central Texas—and also highlighted the extraordinary partnership between local, state, and federal law enforcement that brought the criminals to justice.

Methamphetamine—also known as “meth” and “ice” because it is usually sold in crystallized form—can devastate communities. In a 60-square-mile area of rural Central Texas where the Aryan Brotherhood gang was selling as much as four kilos of the drug each month, meth was taking a toll.

“The area was being tormented,” said Special Agent Dan Snow, who supervises a violent gangs and criminal enterprise squad in the FBI's San Antonio Division. “When you're addicted to meth, you will steal anything that's not bolted down to get money to feed your habit.”

In multiple Central Texas counties near Waco and Fort Hood, crime was spiking—burglaries, property crimes, arsons, assaults, firearms thefts, even homicides—and when local authorities compared notes, they realized that a significant part of the crime problem resulted from the meth trade.

In late 2013, the FBI participated in a meeting with the Texas Department of Public Safety, the Drug Enforcement Agency, and local police departments. “We were hearing from our local counterparts about the issues related to the Aryan Brotherhood,” said Special Agent Dan Tichenor, who investigated the case from the FBI's



regional office in Waco. “From the outset, this investigation was a true partnership between local, state, and federal agencies.”

Through good police work, approximately 30 Aryan Brotherhood gang members central to the drug distribution operation were identified. “The main targets intentionally lived in very rural areas,” Tichenor said, “so law enforcement couldn't do drive-bys of their houses or conduct surveillance. For a time,” he explained, “they were operating under the radar.”

During the course of the three-year investigation, the FBI developed confidential sources and administered court-ordered wire taps. Controlled drug buys were made, and evidence was compiled against the gang members. Eventually, investigators learned the source of the gang's cartel-affiliated supplier in Dallas.

In September 2014, 20 members of the gang were arrested and charged with drug distribution related to the methamphetamine operation. Since then, all 34 Aryan Brotherhood of Texas members who have been charged and convicted for their roles in the

drug network are now serving time in federal prison. On December 9, 2015, Chris Voerhis, 51, was sentenced to 14 years in prison, and Derrick Cooper, 35, received a seven-year term.

“We dismantled their entire organization, from the leadership to suppliers to distributors,” Tichenor said. “This case has had a big impact on the community,” he added. “Local police departments reported a significant drop in crime—especially property crimes—after the drug operation was stopped.”

At the time of Voerhis' and Cooper's sentencings, Special Agent in Charge Christopher Combs of the San Antonio Field Office noted that “these sentences resulted from unprecedented collaboration of federal, state, and local law enforcement.” He added, “This effort not only exemplifies our commitment to prevent gang violence and criminal activity from poisoning our communities, it sends a clear message that we will relentlessly pursue and prosecute the leaders and members of these violent criminal enterprises regardless of where they lay their heads.”



## Index

### ART CRIME

- Art Crime: The Case of the Stolen Stradivarius, pages 10-11
- Art Crime Team Celebrates 10th Anniversary: A Decade of Successful Investigations and Recoveries, pages 16-17
- ISIL and Antiquities Trafficking: FBI Warns Dealers, Collectors About Terrorist Loot, pages 92-93

### CIVIL RIGHTS

- Human Trafficking Ring Dismantled: Case Highlights FBI's Commitment to Anti-Trafficking Efforts, page 12
- Ten Sentenced in Hate Crime Case: Murdered Man Among Multiple Victims, page 61
- Investigating Human Rights: Reaching Out to Diaspora Communities in U.S. for War Crimes Tips, pages 72-73
- Latest Hate Crime Statistics Available: Report Contains Info on Offenses, Victims, and Offenders, pages 130-131
- Human Trafficking: Prison Time for Men Who Attempted to Buy Sex Slaves, page 139

### COUNTERTERRORISM

- New Most Wanted Terrorist: Naturalized U.S. Citizen Born in Somalia Added to FBI List, page 13
- The Oklahoma City Bombing: 20 Years Later, pages 33-44
- Attacks on Arkansas Power Grid: Perpetrator Sentenced to 15 Years, page 88
- ISIL and Antiquities Trafficking: FBI Warns Dealers, Collectors About Terrorist Loot, pages 92-93

Preparing for the Pope: FBI Part of Well-Rehearsed Security Effort, pages 104-105

Symposium Facilitates Research on Lawful Interrogations: Event Sponsored by Government's High-Value Detainee Interrogation Group, pages 118-119

Model Partnership: New York Joint Terrorism Task Force Celebrates 35 Years, page 138

### CRIMES AGAINST CHILDREN

- Help Us Find Them: National Missing Children's Day 2015, page 54
- Sextortion: Help Us Locate Additional Victims of an Online Predator, pages 68-71
- International Parental Kidnapping Case: Partnerships, Publicity Key to 9-Year-Old's Rescue, pages 82-83
- Sexual Predator Sentenced to 29 Years: Targeted Young Victims Through Social Media, page 84
- Cold Case Investigation: Solving a Decades-Old Mystery, pages 85-86
- Operation Cross Country: Recovering Victims of Child Sex Trafficking, pages 112-113
- Operation Northern Spotlight: American-Canadian Partnership Combats Human Trafficking, page 117

### CRIMINAL JUSTICE

#### INFORMATION SERVICES

- Next Generation Crime Stats: UCR's NIBRS Can Offer Fuller Crime Picture, pages 48-49
- Latest Crime Stats Released: Decrease in 2014 Violent Crimes, Property Crimes, page 107

In the Line of Duty: *Law Enforcement Officers Killed and Assaulted*, 2014 Report Released, page 116

Latest Hate Crime Statistics Available: Report Contains Info on Offenses, Victims, and Offenders, pages 130-131

2015 Biometric Identification Award: Virginia Police Investigator Honored for Role in Identifying Violent Perpetrator, page 133

2014 Expanded Crime Statistics Released: National Incident-Based Reporting System Includes More Detailed Data, page 140

### CYBER CRIMES

- Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Threat, pages 8-9
- The Cyber Action Team: Rapidly Responding to Major Computer Intrusions, page 23
- FBI Safe Online Surfing Internet Challenge: Cyber Safety for Young Americans, page 60
- Cyber Criminal Forum Taken Down: Members Arrested in 20 Countries, page 74
- Business E-Mail Compromise: An Emerging Global Threat, pages 94-95
- National Cyber Security Awareness Month: Securing Cyberspace is a Shared Responsibility, pages 108-109

### DIRECTOR/FBI LEADERSHIP

- Law Enforcement and Race: Director Cites 'Hard Truths' and Calls for 'Open Discussion', page 18
- Law Enforcement and Race: Continuing the Conversation, page 24

## Index

Progress Report: Panel Conducts  
Review of FBI Since 9/11  
Commission Report, page 27

Race and Law Enforcement:  
Director Urges Closer Ties  
Between Police, Communities,  
pages 114-115

Symposium Facilitates Research  
on Lawful Interrogations: Event  
Sponsored by Government's  
High-Value Detainee  
Interrogation Group, pages  
118-119

FBI Celebrates 75th Anniversary of  
Legat in Mexico City: Milestone  
Marks Longstanding Crime-  
Fighting Alliance, page 137

Model Partnership: New York Joint  
Terrorism Task Force Celebrates  
35 Years, page 138

### FIELD CASES

Armenian Criminal Enterprise  
Dealt Serious Blow: Cooperative  
Law Enforcement Effort was Key,  
page 6

Extreme Case of Witness  
Intimidation: Justice for Six Slain  
Victims in Philadelphia, page 7

Art Crime: The Case of the Stolen  
Stradivarius, pages 10-11

Human Trafficking Ring  
Dismantled: Case Highlights  
FBI's Commitment to  
Anti-Trafficking Efforts, page 12

New Most Wanted Terrorist:  
Naturalized U.S. Citizen Born in  
Somalia Added to FBI List, page  
13

Drug Kingpin Dethroned:  
International Investigation  
Dismantles Criminal Enterprise,  
page 14

Former Los Alamos Lab Workers  
Sentenced: Nuclear Scientist  
and Wife Passed Classified  
Documents, page 15

A Ponzi Scheme Collapses:  
Financial Crime Ring  
Uncovered, Criminals Brought to  
Justice, page 19

Joint Effort Takes Down Detroit-  
Based Robbery Group: But  
Smash and Grab Jewelry Store  
Incidents are on the Rise, pages  
20-21

License to Steal: Multi-State  
Fraudulent Document Ring  
Dismantled, page 22

Financial Fraud: Hollywood Film  
Scheme Results in Unhappy  
Ending for Investors, page 25

Leader of Violent Street Gang  
Going to Prison: Multi-Agency  
Investigation Dismantles  
Criminal Organization, page 26

Public Corruption: FBI Agent  
Helps Protect His Native  
American Community, page 31

Violent Gangs: Kidnapping Crew  
Targeted Criminal Community,  
page 32

The Oklahoma City Bombing: 20  
Years Later, pages 33-44

Justice for Victims: Restitution  
Ordered in Decade-Long Ponzi  
Scheme, page 45

Profits Over Safety: Egg Company's  
Fraudulent Practices Put Public  
at Risk, page 50

Alabama Jeweler Sentenced in  
Federal Court: Caught Pawning  
His Own 'Stolen' Diamonds,  
page 51

Financial Fraud: Oklahoma Pastor  
Embezzled Nearly \$1 Million  
from Community Center, page 52

Leader of Violent California Gang  
Sentenced: Operations Financed  
Through Drug and Firearms  
Trafficking, page 53

International Soccer Officials  
Indicted: 'Deep-Rooted'  
Corruption, Racketeering

Alleged, page 55

Taken for a Ride: Travel Agent  
Scammed Marching Bands Out  
of Trips, page 56

Financial Fraud: Lengthy Prison  
Term for Advance Fee Fraudster,  
page 57

Serial Armed Robber Gets  
Substantial Prison Term: Joint  
Law Enforcement Effort Pays Off,  
page 58

The Case of the Corrupt Coin  
Dealer: Fraudster Targeted  
Elderly Victims, page 59

Ten Sentenced in Hate Crime  
Case: Murdered Man Among  
Multiple Victims, page 61

Health Care Fraud Takedown:  
243 Arrested, Charged with  
\$712 Million in False Medicare  
Billings, page 62

Multi-State Chop Shop Operation  
Disrupted: Criminal Enterprise  
Leader Among Those Convicted,  
page 63

Behind the Scenes with  
Operational Medics: A Look  
Inside Our Washington Field  
Office's OpMed Program, pages  
64-65

Sextortion: Help Us Locate  
Additional Victims of an Online  
Predator, pages 68-71

Cyber Criminal Forum Taken  
Down: Members Arrested in 20  
Countries, page 74

Financial Fraud: The Hair Show  
That Never Was, page 79

International Parental Kidnapping  
Case: Partnerships, Publicity Key  
to 9-Year-Old's Rescue, pages  
82-83

Sexual Predator Sentenced to 29  
Years: Targeted Young Victims  
Through Social Media, page 84



## Index

Cold Case Investigation: Solving a Decades-Old Mystery, pages 85-86

Byte Out of History: FBI Involvement in Early Election Fraud Case in Kansas City, page 87

Attacks on Arkansas Power Grid: Perpetrator Sentenced to 15 Years, page 88

Loan Sharks Sentenced: Albanian Crime Group Used Violence, Intimidation in Business Dealings, page 89

Former DuPont Employee Sentenced: Involved in Foreign Conspiracy to Steal Trade Secrets, page 90

Medicare Fraud: Hospice Owner Falsified Numerous Claims, page 91

Jewelry Store Robberies: Dallas Task Force Helps Put Violent Criminals Behind Bars, pages 96-97

Steroids Dealer Sentenced: Advertised Products Online, page 98

La Cosa Nostra: Lengthy Prison Terms for Lucchese Crime Family Members, page 99

Man Sentenced for Orchestrating 'Cramming' Scheme: Unauthorized Charges Placed on Victims' Phone Bills, pages 102-103

Preparing for the Pope: FBI Part of Well-Rehearsed Security Effort, pages 104-105

Con Man Sentenced in Fraud Case: Promised Luxury Cars But Rarely Delivered, page 106

Insurance Broker Sentenced for Fraud: Hundreds of Companies Victimized in Multi-State Scheme, page 110

Identity Theft: Fake Hospice Nurse Treated More Than 200 Patients, page 111

Operation Cross Country: Recovering Victims of Child Sex Trafficking, pages 112-113

Financial Fraud: Inside the Investigation of a Las Vegas Construction Boss, pages 120-121

Public Corruption Fugitive Extradited to U.S.: State Official Returns to Face Justice, pages 122-123

Navy Engineer Sentenced for Attempted Espionage: Passed Information on Latest Aircraft Carrier to Undercover Agent, pages 124-125

Solving Homicides: FBI Forms Unique Partnership with Oakland Police Department, pages 126-127

Human Trafficking: Prison Time for Men Who Attempted to Buy Sex Slaves, page 139

New Top Ten Fugitive: Help Us Find a Violent Criminal, page 141

Violent Carjackers Sentenced: Law Enforcement Partnerships Have an Impact, page 142

Drug Trafficking: Aryan Brotherhood Methamphetamine Operation Dismantled, page 143

## FOREIGN

### COUNTERINTELLIGENCE

Former Los Alamos Lab Workers Sentenced: Nuclear Scientist and Wife Passed Classified Documents, page 15

Economic Espionage: FBI Launches Nationwide Awareness Campaign, pages 80-81

Former DuPont Employee Sentenced: Involved in Foreign Conspiracy to Steal Trade Secrets, page 90

Navy Engineer Sentenced for Attempted Espionage: Passed Information on Latest Aircraft Carrier to Undercover Agent, pages 124-125

## HISTORY

The Oklahoma City Bombing: 20 Years Later, pages 33-44

The FBI Website at 20: Two Decades of Fighting Crime and Terrorism, pages 66-67

Cold Case Investigation: Solving a Decades-Old Mystery, pages 85-86

Byte Out of History: FBI Involvement in Early Election Fraud Case in Kansas City, page 87

Newseum Goes "Inside Today's FBI": D.C. Museum Updates Popular Exhibit, pages 128-129

Agents of Asian Ancestry: 'Historical Marker' Celebrates 50 Years of Service, pages 134-135

FBI Celebrates 75th Anniversary of Legat in Mexico City: Milestone Marks Longstanding Crime-Fighting Alliance, page 137

Model Partnership: New York Joint Terrorism Task Force Celebrates 35 Years, page 138

## INTELLIGENCE

National Explosives Task Force: A Multi-Agency Group of Bomb Experts, page 30

Symposium Facilitates Research on Lawful Interrogations: Event Sponsored by Government's High-Value Detainee Interrogation Group, pages 118-119

## Index

### INTERNATIONAL

New Most Wanted Terrorist:  
Naturalized U.S. Citizen Born in  
Somalia Added to FBI List, page  
13

Drug Kingpin Dethroned:  
International Investigation  
Dismantles Criminal Enterprise,  
page 14

FBI Establishes International  
Corruption Squads: Targeting  
Foreign Bribery, Kleptocracy  
Crimes, pages 28-29

International Soccer Officials  
Indicted: 'Deep-Rooted'  
Corruption, Racketeering  
Alleged, page 55

Investigating Human Rights:  
Reaching Out to Diaspora  
Communities in U.S. for War  
Crimes Tips, pages 72-73

Cyber Criminal Forum Taken  
Down: Members Arrested in 20  
Countries, page 74

International Law Enforcement  
Training: Celebrating 20 Years  
of Partnership and Excellence,  
pages 75-78

Economic Espionage: FBI  
Launches Nationwide Awareness  
Campaign, pages 80-81

International Parental Kidnapping  
Case: Partnerships, Publicity Key  
to 9-Year-Old's Rescue, pages  
82-83

ISIL and Antiquities Trafficking:  
FBI Warns Dealers, Collectors  
About Terrorist Loot, pages  
92-93

Business E-Mail Compromise: An  
Emerging Global Threat, pages  
94-95

Operation Northern Spotlight:  
American-Canadian Partnership  
Combats Human Trafficking,  
page 117

International Operations: Building  
Partnerships in the Americas,  
page 132

FBI Celebrates 75th Anniversary of  
Legat in Mexico City: Milestone  
Marks Longstanding Crime-  
Fighting Alliance, page 137

### MAJOR THEFTS/VIOLENT CRIME

Extreme Case of Witness  
Intimidation: Justice for Six Slain  
Victims in Philadelphia, page 7

Art Crime: The Case of the Stolen  
Stradivarius, pages 10-11

Joint Effort Takes Down Detroit-  
Based Robbery Group: But  
Smash and Grab Jewelry Store  
Incidents are on the Rise, pages  
20-21

Leader of Violent Street Gang  
Going to Prison: Multi-Agency  
Investigation Dismantles  
Criminal Organization, page 26

Violent Gangs: Kidnapping Crew  
Targeted Criminal Community,  
page 32

Alabama Jeweler Sentenced in  
Federal Court: Caught Pawning  
His Own 'Stolen' Diamonds,  
page 51

Leader of Violent California Gang  
Sentenced: Operations Financed  
Through Drug and Firearms  
Trafficking, page 53

Serial Armed Robber Gets  
Substantial Prison Term: Joint  
Law Enforcement Effort Pays Off,  
page 58

Multi-State Chop Shop Operation  
Disrupted: Criminal Enterprise  
Leader Among Those Convicted,  
page 63

Cold Case Investigation: Solving  
a Decades-Old Mystery, pages  
85-86

Business E-Mail Compromise: An  
Emerging Global Threat, pages  
94-95

Jewelry Store Robberies: Dallas  
Task Force Helps Put Violent  
Criminals Behind Bars, pages  
96-97

Latest Crime Stats Released:  
Decrease in 2014 Violent Crimes,  
Property Crimes, page 107

Identity Theft: Fake Hospice Nurse  
Treated More Than 200 Patients,  
page 111

In the Line of Duty: *Law  
Enforcement Officers Killed and  
Assaulted*, 2014 Report Released,  
page 116

Solving Homicides: FBI Forms  
Unique Partnership with  
Oakland Police Department,  
pages 126-127

2015 Biometric Identification  
Award: Virginia Police  
Investigator Honored for Role in  
Identifying Violent Perpetrator,  
page 133

2014 Expanded Crime Statistics  
Released: National Incident-  
Based Reporting System Includes  
More Detailed Data, page 140

New Top Ten Fugitive: Help Us  
Find a Violent Criminal, page  
141

Violent Carjackers Sentenced: Law  
Enforcement Partnerships Have  
an Impact, page 142

### ORGANIZED CRIME/DRUGS

Armenian Criminal Enterprise  
Dealt Serious Blow: Cooperative  
Law Enforcement Effort was Key,  
page 62

Human Trafficking Ring  
Dismantled: Case Highlights  
FBI's Commitment to  
Anti-Trafficking Efforts, page 12



## Index

Drug Kingpin Dethroned:  
International Investigation  
Dismantles Criminal Enterprise,  
page 14

License to Steal: Multi-State  
Fraudulent Document Ring  
Dismantled, page 22

Leader of Violent Street Gang  
Going to Prison: Multi-Agency  
Investigation Dismantles  
Criminal Organization, page 26

Leader of Violent California Gang  
Sentenced: Operations Financed  
Through Drug and Firearms  
Trafficking, page 53

International Soccer Officials  
Indicted: 'Deep-Rooted'  
Corruption, Racketeering  
Alleged, page 55

Multi-State Chop Shop Operation  
Disrupted: Criminal Enterprise  
Leader Among Those Convicted,  
page 63

Loan Sharks Sentenced: Albanian  
Crime Group Used Violence,  
Intimidation in Business  
Dealings, page 89

Steroids Dealer Sentenced:  
Advertised Products Online,  
page 98

La Cosa Nostra: Lengthy Prison  
Terms for Lucchese Crime Family  
Members, page 99

Drug Trafficking: Aryan  
Brotherhood Methamphetamine  
Operation Dismantled, page 143

### PARTNERSHIPS

National Explosives Task Force: A  
Multi-Agency Group of Bomb  
Experts, pages 30-31

Death Notification with  
Compassion: FBI Teams Up  
with Penn State to Offer Online  
Training, page 46

Serial Armed Robber Gets  
Substantial Prison Term: Joint  
Law Enforcement Effort Pays Off,  
page 58

Health Care Fraud Takedown:  
243 Arrested, Charged with  
\$712 Million in False Medicare  
Billings, page 62

Investigating Human Rights:  
Reaching Out to Diaspora  
Communities in U.S. for War  
Crimes Tips, pages 72-73

Cyber Criminal Forum Taken  
Down: Members Arrested in 20  
Countries, page 74

International Law Enforcement  
Training: Celebrating 20 Years  
of Partnership and Excellence,  
pages 75-78

International Parental Kidnapping  
Case: Partnerships, Publicity Key  
to 9-Year-Old's Rescue, pages  
82-83

Preparing for the Pope: FBI Part of  
Well-Rehearsed Security Effort,  
pages 104-105

Operation Cross Country:  
Recovering Victims of Child Sex  
Trafficking, pages 112-113

Operation Northern Spotlight:  
American-Canadian Partnership  
Combats Human Trafficking,  
page 117

Symposium Facilitates Research  
on Lawful Interrogations: Event  
Sponsored by Government's  
High-Value Detainee  
Interrogation Group, pages  
118-119

Solving Homicides: FBI Forms  
Unique Partnership with  
Oakland Police Department,  
pages 126-127

Newseum Goes "Inside Today's  
FBI": D.C. Museum Updates  
Popular Exhibit, pages 128-129

International Operations: Building  
Partnerships in the Americas,  
page 132

2015 Biometric Identification  
Award: Virginia Police  
Investigator Honored for Role in  
Identifying Violent Perpetrator,  
page 133

FBI Celebrates 75th Anniversary of  
Legat in Mexico City: Milestone  
Marks Longstanding Crime-  
Fighting Alliance, page 137

Model Partnership: New York Joint  
Terrorism Task Force Celebrates  
35 Years, page 138

Violent Carjackers Sentenced: Law  
Enforcement Partnerships Have  
an Impact, page 142

### PUBLIC/COMMUNITY OUTREACH

Adopt-A-School Program, Part 1:  
Bringing a Message of Hope to  
Students, page 1

Adopt-A-School Program, Part  
2: Becoming a Junior Special  
Agent, pages 2-3

Adopt-A-School Program, Part 3:  
'I Promise to be a Good Citizen',  
pages 4-5

New Most Wanted Terrorist:  
Naturalized U.S. Citizen Born in  
Somalia Added to FBI List, page  
13

Law Enforcement and Race:  
Director Cites 'Hard Truths' and  
Calls for 'Open Discussion', page  
18

Law Enforcement and Race:  
Continuing the Conversation,  
page 24

Community Partners Recognized:  
2014 Director's Community  
Leadership Awards, page 47

Help Us Find Them: National  
Missing Children's Day 2015,  
page 54

## Index

FBI Safe Online Surfing Internet Challenge: Cyber Safety for Young Americans, page 60

The FBI Website at 20: Two Decades of Fighting Crime and Terrorism, pages 66-67

Community Outreach: Director Comey Praises Citizens Academy Alumni Association, pages 100-101

National Cyber Security Awareness Month: Securing Cyberspace is a Shared Responsibility, pages 108-109

Race and Law Enforcement: Director Urges Closer Ties Between Police, Communities, pages 114-115

Newseum Goes “Inside Today’s FBI”: D.C. Museum Updates Popular Exhibit, pages 128-129

Want to Obtain FBI Records a Little Quicker?: Try New eFOIA System, page 136

New Top Ten Fugitive: Help Us Find a Violent Criminal, page 141

### PUBLIC CORRUPTION

Public Corruption: FBI Agent Helps Protect His Native American Community, page 31

Profits Over Safety: Egg Company’s Fraudulent Practices Put Public at Risk, page 50

Byte Out of History: FBI Involvement in Early Election Fraud Case in Kansas City, page 87

Financial Fraud: Inside the Investigation of a Las Vegas Construction Boss, pages 120-121

Public Corruption Fugitive Extradited to U.S.: State Official Returns to Face Justice, pages 122-123

### RECRUITING/DIVERSITY

Agents of Asian Ancestry: ‘Historical Marker’ Celebrates 50 Years of Service, pages 134-135

### TECHNOLOGY

Want to Obtain FBI Records a Little Quicker?: Try New eFOIA System, page 136

### TRAINING

Death Notification with Compassion: FBI Teams Up with Penn State to Offer Online Training, page 46

Behind the Scenes with Operational Medics: A Look Inside Our Washington Field Office’s OpMed Program, pages 64-65

International Law Enforcement Training: Celebrating 20 Years of Partnership and Excellence, pages 75-78

### WHITE-COLLAR CRIME

A Ponzi Scheme Collapses: Financial Crime Ring Uncovered, Criminals Brought to Justice, page 19

Financial Fraud: Hollywood Film Scheme Results in Unhappy Ending for Investors, page 25

FBI Establishes International Corruption Squads: Targeting Foreign Bribery, Kleptocracy Crimes, pages 28-29

Justice for Victims: Restitution Ordered in Decade-Long Ponzi Scheme, page 45

Profits Over Safety: Egg Company’s Fraudulent Practices Put Public at Risk, page 50

Financial Fraud: Oklahoma Pastor Embezzled Nearly \$1 Million from Community Center, page 52

International Soccer Officials Indicted: ‘Deep-Rooted’ Corruption, Racketeering Alleged, page 55

Taken for a Ride: Travel Agent Scammed Marching Bands Out of Trips, page 56

Financial Fraud: Lengthy Prison Term for Advance Fee Fraudster, page 57

The Case of the Corrupt Coin Dealer: Fraudster Targeted Elderly Victims, page 59

Health Care Fraud Takedown: 243 Arrested, Charged with \$712 Million in False Medicare Billings, page 62

Financial Fraud: The Hair Show That Never Was, page 79

Medicare Fraud: Hospice Owner Falsified Numerous Claims, page 91

La Cosa Nostra: Lengthy Prison Terms for Lucchese Crime Family Members, page 99

Man Sentenced for Orchestrating ‘Cramming’ Scheme: Unauthorized Charges Placed on Victims’ Phone Bills, pages 102-103

Con Man Sentenced in Fraud Case: Promised Luxury Cars But Rarely Delivered, page 106

Insurance Broker Sentenced for Fraud: Hundreds of Companies Victimized in Multi-State Scheme, page 110

Identity Theft: Fake Hospice Nurse Treated More Than 200 Patients, page 111

Financial Fraud: Inside the Investigation of a Las Vegas Construction Boss, pages 120-121









## FBI OFFICE OF PUBLIC AFFAIRS

935 Pennsylvania Avenue NW

Washington, D.C. 20535



The FBI's Office for Victim Assistance (OVA) introduced two new Crisis Response K-9s to its team in October 2015. Gio and Wally (seen in background on left), with their docile temperaments, can help calm and comfort victims during emotionally trying situations. The dogs, both Labrador retrievers, are part of OVA's efforts to help victims cope with the impact of crime.