



THE FBI STORY

2016



Joint Interagency Task Force South personnel operate aboard a U.S. Navy plane to track drug traffickers.

THE FBI STORY

2016

www.fbi.gov



The Joint Interagency Task Force South, or JIATF-S, is located within a naval air station on Key West, Florida. The task force, created nearly three decades ago, is composed of every branch of the U.S. military, U.S. federal intelligence and law enforcement agencies, and 15 partner nations. (page 128)

A Message from FBI Director James B. Comey

For the FBI, 2016 was a demanding year as we carried out our mission: to protect the American people and uphold the Constitution of the United States. Working with our law enforcement and intelligence partners at home and abroad, we shielded innocent people from terrorist attacks, cyber intrusions, spies, and other national security threats. We locked up human traffickers, child pornographers, corrupt public officials, and fraudsters. And we helped neighborhoods break free from the grip of gangs and drugs.

This latest edition of *The FBI Story*, our annual collection of news and feature articles from the Bureau's public website, offers a glimpse of the challenges we faced. Here you can read about some of our most successful recent investigations and operations. These include a nationwide child exploitation sweep that recovered 82 young victims; the dismantling of the vast Avalanche cyber crime network, which gave criminals an unfettered platform to target victims worldwide with malware; and the capture and conviction of a foreign "seed spy," who stole patented corn seeds that contained valuable agricultural trade secrets of American companies.

This edition of *The FBI Story* also features some of the Bureau's extraordinary capabilities. You will learn how the talented people of the FBI Laboratory create facial approximations of unidentified remains to help local investigators solve crimes. You will discover how our Victim Assistance Rapid Deployment Team and Crisis Response Canines help crime victims cope with tragedy. And you will read about our Weapons of Mass Destruction Directorate, which works to stop all kinds of twisted people seeking to bomb, poison, and sicken the innocent. You will also find articles on FBI history, including a feature on how the Bureau has evolved in the 15 years since the 9/11 attacks.

Looking ahead to 2017 and beyond, we know our work will only grow more challenging. Yet as these stories make clear, the FBI doesn't face these threats alone. We rely on the strong partnerships we have built over many decades with law enforcement, intelligence agencies, the private sector, and citizens from all walks of life. The amazing work you will read about in these pages would be impossible without the trust and confidence of the American people.

On behalf of the entire Bureau, I thank you for your support of the FBI, and I hope you will enjoy this latest edition of *The FBI Story*.

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.



Recipients of the 2015 Director's Community Leadership Awards were celebrated at FBI Headquarters in Washington, D.C. on April 15, 2016. (page 39)

Fool's Gold

Company That Enabled Get-Rich-Quick Schemes Left Many High and Dry

The recent announcement that federal authorities have returned nearly \$12 million in recovered losses to more than 1,000 victims of an elaborate fraud scheme represents still another cautionary reminder that all that glitters is not gold.

For nearly seven years, Goldfinger Coin & Bullion operated a website that purported to provide an easy way for customers to invest in precious metals. Users could buy, hold, and transfer gold and silver on the California company's online platform, e-Bullion.com, and convert their holdings to cash at ATMs around the world. With gold's market value steadily rising, the operation seemed like a lucrative bet.

But as investigators discovered in 2008, the company was doing much more than trading in precious metals. Without a license, Goldfinger was operating almost solely as a money-transmitter, earning owners Jim and Pamela Fayed millions from fees on users' transactions. The e-Bullion website touted no fees for establishing or funding an account, but there was a cost for converting virtual holdings back into real money. FBI and IRS investigators determined that about \$35 million per month funneled through Goldfinger and e-Bullion at the company's height, and very little of it came from trading precious metals.

"That's how we knew it wasn't a gold dealer," said Special Agent Maura Kelley, who worked in the FBI's Ventura County office (before retiring last year) and investigated the case jointly with the IRS and the U.S. Attorney's Office for the Central District of California. "Typically, if you're a gold dealer, you buy it and you hold it. You

don't buy and sell, because there's no money to be made. There should have been a lot of money coming in and little going out, unless it was to buy gold. And that wasn't happening."

Instead, investigators said, e-Bullion—with more than one million users—was reaping huge profits on transaction fees, mostly related to illegal activities like Ponzi schemes (see sidebar). Had the company been properly licensed, it would have had to comply with strict reporting requirements, such as filing suspicious activity reports on sketchy transactions and so-called high-yield investment programs. Not only was the company circumventing the rules, it was scooping up money left behind in e-Bullion accounts when the Ponzi schemes collapsed and the operators disappeared.

"He just pocketed the money from all these high-yield investment programs after they ran," Kelley said, referring to Jim Fayed. "And the money continued to come in because the word didn't get out right away that they weren't paying. And people were still investing."

The FBI and IRS shut down the company in 2008 following the murder of co-founder Pamela Fayed and the subsequent arrest of Jim Fayed, who had hired the hitmen who killed her. He is currently on death row in California.

Investigators spent months following the digital money trail and tracking down the company's gold holdings in Los Angeles and Perth, Australia. Last year, the government returned \$1.8 million to more than 300 victims of one particular illegal scheme called Kum Ventures that was run through e-Bullion. In November,

\$11.7 million in civilly forfeited proceeds was distributed back to victims in the U.S., Canada, and Australia. Another \$12 million in precious metals in Australia that belonged to Fayed is pending repatriation to the U.S. to be returned to e-Bullion victims.

Kelley spent nearly 30 years working white-collar crime cases for the FBI, including many like the Ponzi schemes that led back to e-Bullion. Ponzi schemes appear in different forms, but they always make the same promise of quick returns. And they always end with a crash.

"They take the money and run," Kelley said. "They don't look back."

Ponzi schemes promise high financial returns or dividends not available through traditional investments. Instead of investing the funds of victims, however, the con artists pay "dividends" to initial investors using the funds of subsequent investors. The schemes generally fall apart when the operators flee with the proceeds or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."

This type of fraud is named after Charles Ponzi of Boston, Massachusetts. In the early 1900s, Ponzi launched a scheme that guaranteed investors a 50 percent return on their investment in postal coupons. Although he was able to pay his initial backers, the scheme dissolved when he was unable to pay later investors.

Tips for Avoiding Ponzi Schemes

- Be careful of any investment opportunity that makes exaggerated earnings claims.
- 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.

Transnational Gangs

Part 1: Understanding the Threat

The town of Sonsonate, not far from the Pacific Ocean in western El Salvador, is home to a prison housing more than 800 inmates. Like many of the prisons in this Central American country, Centro Penal De Sonsonate incarcerates only gang members—and, by definition, each one is a killer.

La Mara Salvatrucha, or MS-13, and the 18th Street gang require their mostly teenage recruits to undergo at least two years of initiation before becoming full-fledged gang members. One of the final tests for membership is to commit murder.

“That is certain, you have to kill,” said Special Agent Julian Iguilada, who is part of an FBI team that works in El Salvador with local law enforcement and the government to fight the transnational gang threat, because what happens there—and elsewhere in Central America—has a significant impact

on the safety of U.S. citizens at home and abroad. Gang leaders in El Salvador routinely order their subordinates to commit crimes, including murder, on U.S. soil—and many times these orders are issued from behind bars.

“El Salvador has become the epicenter of gang violence in Central America and represents the largest connection to gang crime in the U.S.,” said Special Agent Grant Mann, who works in the Safe Streets and Gang Unit at FBI Headquarters in Washington and helps U.S. and Central American law enforcement agencies forge partnerships in the battle against transnational gangs.

“The gangs respect no borders, so law enforcement must respond in kind by working together,” Mann said. His unit recently sponsored a Central American Law Enforcement Exchange (CALEE) that brought Central

American police officers and prosecutors together with local law enforcement personnel from American cities where MS-13 and 18th Street operate. It was the sixth such exchange the FBI has sponsored jointly with the U.S. Department of State since 2009. The goal of CALEE is to have participants share intelligence about the gangs as well as best practices.

The MS-13 and 18th Street gangs have become so bloodthirsty in El Salvador that the government has declared them terrorist organizations. The gangs are responsible for bringing the murder rate to a level last seen during the 1979-1992 civil war.

Last year during the month of August, there were 907 murders in El Salvador, a small country roughly the size of Massachusetts. By comparison, Chicago—known



A look at the joint training of police officers from select Central American countries and U.S. cities. The annual Central American Law Enforcement Exchange includes a week in El Salvador, the so-called “epicenter of gang violence,” where the street gangs MS-13 and 18th Street are regarded as terrorist organizations.

for its gang violence—recorded 411 murders during the entire year in 2014, according to the FBI's Uniform Crime Report. In 2015 in El Salvador, 55 police officers were assassinated by the gangs, along with 18 military officers, six corrections officers, one prosecutor, and one judge.

"In El Salvador now, we have a murder rate of 25 per day, and 80 percent is gang related," Iguarada said. "Many of the gang members committing these homicides are 13-, 14-, and 15-year-olds," he explained, "and every day there are new members coming in."

"We aren't facing a group of youths who are rebelling, but a very structured organization conducting criminal activities," said Luis Martinez, El Salvador's attorney general and the country's highest ranking law enforcement officer. "They are using military-grade weapons, and they are using them

against the police, military, and prosecutors."

MS-13 and 18th Street gang members have gained a foothold in numerous U.S. cities, including Los Angeles, Boston, Houston, Charlotte, Newark, and the Northern Virginia suburbs of Washington, D.C. They commit a variety of crimes—mainly trafficking drugs and extorting individuals and business owners—and they maintain strong ties to Central America.

Although gang members in both countries are tightly aligned, Iguarada pointed out that they differ in subtle ways. "A big difference in El Salvador is that gang members don't see the gang as a way to make money, to buy the fancy car or house," he said. "They are in the gang to belong to a social group. They see the gang as a father figure, as a mother figure. They are in the gang because they

want to be, and they do what the gang asks them to do."

"For the gangs, loyalty is key," Iguarada added. "Once you come into the gang, you don't have a family anymore. The gang is your family. And when you get in, with few exceptions, you get in for life. And it's a life of crime and violence."

About This Series

Since 2009, the FBI and the U.S. Department of State have sponsored the Central American Law Enforcement Exchange (CALEE), which brings Central American police officers and prosecutors together with law enforcement personnel from U.S. cities where violent gangs like MS-13 and 18th Street operate. In this three-part series, FBI.gov looks at how cooperative efforts are yielding mutual benefits in the fight against transnational gangs.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/transnationalgangs.



The gang La Mara Salvatrucha, or MS-13, makes its presence known in the town of Sonsonate.

Transnational Gangs

Part 2: Countering the Threat with Strong Partnerships



FBI personnel provided tactical training in Houston during the second week of the three-week Central American Law Enforcement Exchange, or CALEE.

At the start of the FBI's recent Central American Law Enforcement Exchange (CALEE) program, participants from U.S. police departments and their counterparts from Mexico, El Salvador, Honduras, Guatemala, Belize, and Panama were strangers, but they shared one thing in common: a commitment to make their communities safe from violent gangs such as MS-13 and 18th Street.

By the end of the three-week program, the men and women had overcome language barriers and become friends as well as partners—and they were armed with new resources to fight the transnational gang threat: a network of intelligence sharing, expanded contacts, and access to FBI-led task forces throughout Central America.

"There's a synergy between the gangs that helps them grow and become stronger," said Special Agent Jason Kaplan, the FBI's legal

attaché in El Salvador. "As law enforcement, we need to develop that same relationship with each other, because the gangs are doing it, and if we don't we are going to fall behind."

CALEE was developed in 2009 with that spirit of collaboration and partnership in mind. This year's group of nearly 40 participants traveled to Los Angeles and Houston before spending a final week in El Salvador, where the MS-13 and 18th Street gangs have grown powerful and extremely violent. In each venue, participants received training and information about different jurisdictions' approaches to managing their gang threat.

In El Salvador, besides getting a first-hand look at gang neighborhoods and a prison whose inmates are exclusively violent gang members, participants were briefed on the latest cases and trends within the gangs. Many MS-13 and 18th Street leaders—some of whom

are incarcerated—are located in Central America and order crimes to be committed in the United States.

CALEE participants also learned about the Transnational Anti-Gang Task Forces (TAGs), in which FBI agents are embedded with vetted Central American police officers to work cases and gather intelligence. Currently there are TAGs in El Salvador, Guatemala, and Honduras. They have been in existence for more than five years, and they are highly successful.

"Before the Transnational Anti-Gang Task Forces were set up," Kaplan explained, "gang investigations in the United States that led to subjects in these countries often came to a dead end. There was no mechanism for us to really further those investigations." Since the TAGs were established, he said, "we now have a liaison here, a resource for investigators in the United States. When they get to that point where they realize



Gang graffiti in El Salvador.



The seal for the Transnational Anti-Gang Task Force, or TAG.

that one of their principal subjects is located in Central America, they now have resources where they can go to further that investigation. Similarly, the countries of El Salvador, Guatemala, and Honduras can do the same.”

Kaplan added that intelligence gathered by the TAGs has stopped crimes—including murders—from taking place. “Dozens of lives, possibly hundreds, have been saved since the establishment of the anti-gang task forces.”

“Certainly the value of the TAGs can’t be understated,” noted Special Agent Grant Mann, who works in the Safe Streets and Gang Unit at FBI Headquarters in Washington, D.C. and helped organize this year’s CALEE program. “One of our main goals for the group in El Salvador was to fully expose participants to what the FBI has here by way of resources.”

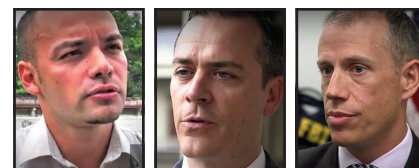
Mann’s unit also administers the FBI’s Safe Streets Violent Crime Initiative. Established in 1992, the

program is designed to bring local, state, and federal law enforcement together in their U.S. communities to fight gang-related crime. Today there are 164 Safe Streets Task Forces throughout the country, and U.S. CALEE participants are drawn from the ranks of Safe Streets Task Force officers.

“The Safe Streets model combines the strengths of all these different agencies and all of our FBI resources,” Mann said. “The goal is to make everyone’s community safer. Our efforts with the TAGs and our international partners are an extension of that goal, because there is no doubt that the gang problems in El Salvador have an impact on gang crime in the U.S.”

Speaking of the cooperative efforts between the U.S. and El Salvador to fight the MS-13 and 18th Street gangs, El Salvador’s Attorney General Luis Martinez noted, “There is something very important that both countries are aware of: that we share the same serious

problem and that we have to work jointly in order to find resolutions. That is why an event like CALEE 2015 is very important,” he said. “This training will be very valuable for every single participant here.”



(L-R) FBI agents Julian Iguilada, Grant Mann, and Jason Kaplan work with international law enforcement partners to combat the transnational gang threat.

Transnational Gangs

Part 3: Investigators and Prosecutors Join Forces



CALEE participants attend a lecture in El Salvador.

The success of the Central American Law Enforcement Exchange (CALEE) program hinges on bringing together U.S. and Central American law enforcement officers who share a common cause in the fight against violent transnational gangs. During the most recent CALEE, an important new partner was added to the group—prosecutors.

“We have seen that when prosecutors and investigators work together from the outset, cases tend to have more successful outcomes,” said Special Agent Grant Mann, who helped plan and administer CALEE 2015, the sixth session since the program began in 2009.

In the U.S., it is typical for FBI agents and prosecutors to sit down at the beginning of an investigation

to discuss possible charges and investigative strategies. Historically, that collaborative process is less common in Central America—but thanks to programs such as CALEE, it is gaining acceptance.

During the recent three-week training program focusing on transnational gangs MS-13 and 18th Street, a federal prosecutor from Los Angeles who specializes in gang cases briefed the approximately 40 CALEE participants about recent prosecutions and investigative techniques in his jurisdiction, and he traveled with the group from Los Angeles to Houston and then to El Salvador.

El Salvador Attorney General Luis Martinez assigned prosecutors to brief the group in San Salvador

and embraced the concept of his office and the police working together from the beginning of an investigation. “Gang members are terrorists who have penetrated our institutions,” he said. “We have to fight this for a better future, for the well being of our families.”

Also in attendance during the El Salvador portion of CALEE was Sean Torriente, a U.S. Department of Justice (DOJ) prosecutor who is part of a special program in Central America. “I am in El Salvador working with the local police, prosecutors, and judges to help develop their judicial system,” he said. “The mission is to strengthen the rule of law within El Salvador and also to establish partnerships with local police, prosecutors, and judges that will be beneficial to U.S. cases.”



El Salvador Attorney General Luis Martinez during the CALEE training last September.

Torriente is part of DOJ's Office of Overseas Prosecutorial Development and Training (OPDAT). "We work with anti-gang prosecutors in El Salvador on their cases," he said. "We mentor them on techniques that have worked on our cases, with the idea that the things that work for us in the U.S. may work for them. And they help us build our cases as well."

There are currently three OPDAT prosecutors in Central America. "Most of the crimes here—whether drug trafficking, extortions, or murders—have some kind of gang involvement, Torriente said." What the OPDAT program is doing, he added, "is setting a good example of how close relationships with police and prosecutors can help benefit cases. So far, it's been a great success."

Since the first CALEE six years ago, approximately 300 U.S. and Central American police officers have trained together and become part of a network that share information and help each other with transnational gang cases. Now, with the addition of prosecutors, that network is expanding.

Nearing the close of the most recent session, FBI Special Agent Julian Igualada, who works gang cases in El Salvador, noted that CALEE participants "will depart El Salvador in a few days with a better understanding of what it takes to investigate these international criminal matters committed by the gangs. They will also have the ability to reach out to officers who do the same thing in Panama, Guatemala, Honduras, Belize, Mexico, and the United States," he said. "Being able to exchange

information will help them disrupt and dismantle these criminal organizations."

Mauricio Ramírez Landaverde, director general of El Salvador's National Civilian Police, has participated in every CALEE session and is a strong supporter of the international alliance to fight transnational gangs.

Because of the cooperation among governments and FBI assistance with training and the Transnational Anti-Gang Task Forces, Landaverde explained, "there is an exchange of information going on constantly. Not only can we resolve our own cases, we can collaborate—for example, to search for fugitives and capture them—on whatever is important to each country."

"We are very thankful for this cooperation," he said, adding that in the fight against the gangs, "it is one of the most important tools that we have."



Mauricio Ramírez Landaverde, director general of El Salvador's National Civilian Police.

Financial Fraud

The Disney Resort That Never Was



Thomas W. Lucas, Jr. was such an effective liar that he was able to convince hundreds of investors—even members of his own family—that he had inside information about a Disney resort to be built in Texas that would make the nearby scrubland worth a fortune for those who bought it ahead of time.

Of course, there was no “Frontier Disney,” as Lucas claimed, but using false documents, forged signatures, and phony presentations, he was able to pocket nearly \$450,000 in real estate fees over a four-year period and cause investors to lose approximately \$20 million.

“Thomas Lucas, Jr. fooled savvy investors and very intelligent people,” said Special Agent Rick Velasquez, who investigated the case from the FBI’s Dallas Division. “He was a very believable guy.”

From 2006 to 2010, Lucas defrauded more than 250 investors. He claimed to have insider information regarding a Disney resort and theme park planned for a rural area about 50 miles north of Dallas. He was giving investors a chance to buy surrounding

land outright, or to purchase options to buy the land near the supposed resort. The 65 investors who purchased options lost every cent they invested—more than \$8 million. Some investors, including Lucas’ father and uncle in the family real estate business, purchased land outright, believing the Disney story.

“There was not one grain of truth in Lucas’ presentations,” Velasquez said, “but his pitch was very elaborate, and it fooled a lot of people. He duped his own family.”

Lucas claimed to have letters between Disney and a management firm saying that the company had acquired enough land to make the deal happen. He included the letters—complete with forged Disney officials’ signatures—in his presentations to investors, along with detailed maps, concept plans, and images that were later discovered to be lifted from the Internet, some from Disney websites.

According to Lucas, Disney planned to make the big announcement about the resort at a Dallas Cowboys football game on Thanksgiving in 2006.

When that didn’t happen, he told investors there were delays. “Then the announcement was going to be Super Bowl 2007, 2008. Then it was Fourth of July at the Beijing Olympic games,” Velasquez said. “He was just trying to keep investors and potential investors on the hook.”

With each delay, Lucas would sweeten the pot with some new bogus e-mail from a Disney executive or other bit of tantalizing information meant to persuade people the project was still on track. Eventually, investors became suspicious, and one made a complaint to the FBI.

Velasquez, who specializes in financial fraud cases, says the scheme went on for so long because Lucas was believable—and also because investors could not resist the temptation of making large returns on their money.

When confronted by investigators about his claims, Lucas falsely blamed the supposed Disney information he received on a man he met at a methadone rehab clinic, who had since died. In 2014, Lucas was indicted by a federal grand jury on seven counts of wire fraud and one count of lying to the FBI.

Last September, after a jury trial in which Lucas maintained his innocence but was found guilty on all charges, a judge sentenced the 35-year-old to 17.5 years in prison. “That was a stiff sentence for a white-collar crime,” Velasquez noted, “but he defrauded a lot of people and showed no remorse.”

Countering the Growing Intellectual Property Theft Threat

Enhancing Ties Between Law Enforcement and Business

In 2008, a new federal law creating stricter penalties for criminals who engaged in intellectual property theft was enacted to keep pace with globalization, e-commerce, and technology advances.

Fast forward to 2016: Technological advances continue at an even faster pace, dramatically increasing the threat posed by criminals who steal trade secrets, produce and/or traffic in counterfeit products, and infringe on copyrights. One important factor in this increase is the global expansion of online marketplaces, which aids international and domestic criminal organizations in trafficking in counterfeit goods.

The Department of Justice (DOJ) recently announced a new strategy that involves partnering more closely with businesses in an effort to combat these types of crimes more effectively. Said Attorney General Loretta Lynch, “Through this new approach, we intend to provide information and resources to individuals and companies that will help them identify and disrupt attempts on their intellectual property, extend greater protection to American commerce as a whole, and safeguard the health and safety of individual Americans.”

And the FBI—working with its investigative partners at the National Intellectual Property Rights Coordination Center (NIPRCC)—will play an integral part in this strategy.

The Bureau has already been collaborating for years with brand owners, copyright holders, and trademark holders because we know the harm that intellectual property theft causes: legitimate businesses lose billions of dollars

in revenue and suffer damaged reputations, consumer prices go up, the U.S. and global economies are robbed of jobs and tax revenue, product safety is reduced, and sometimes lives are even put at risk. FBI efforts with these businesses to date have involved shared information, aggressive criminal initiatives based on current or emerging trends, and investigations.

Under the FBI’s new strategy, we’re expanding our efforts to work with third-party entities—such as online marketplaces, payment service providers, and advertisers—that may inadvertently enable the activities of criminals.

- Third-party online marketplaces draw consumers to their sites with competitive pricing and a sense of security, but criminal counterfeiters exploit these marketplaces to gain an appearance of legitimacy, access to far-reaching advertising, and efficient sales transactions.
- Payment service providers—such as credit card payment processors and related payment alternatives—also give counterfeiters the appearance of legitimacy when they provide payment options that consumers mistakenly interpret to mean that the businesses they service are legitimate.
- Online advertising systems and platforms enable website owners to outsource the process of monetizing their website traffic. Criminals have begun exploiting advertising as an alternative revenue stream, drawing traffic to their sites by offering counterfeit products for sale or pirated digital content for download.

The benefits of working with these third-party entities? According to David Farquhar, who heads up the Bureau’s Intellectual Property and Cyber-Enabled Crimes Unit at the NIPRCC, “We’re not only broadening awareness of the crime problem, we can also obtain information about crime trends, get investigative leads that will help us identify criminals, and collect evidence of criminal activity.” Farquhar added that the FBI will assist these companies with refining their own analytical tools and techniques for uncovering fraud.

Also new in our approach to intellectual property theft is an enhanced relationship between our criminal and counterintelligence personnel when working theft of trade secrets cases. A trade secrets case worked under the counterintelligence program—which occurs when the involvement of state-sponsored actors is suspected—will be referred to a criminal squad if no state sponsorship is found. And when criminal investigators begin to suspect the involvement of a state sponsor, the case will be referred to the counterintelligence squad. Our goal is to contain and/or even prevent the theft as quickly as possible, no matter who’s behind it.

The FBI—in partnership with DOJ, the NIPRCC, and law enforcement agencies in the U.S. and abroad—will continue to place a premium on intellectual property theft and strive to find new and effective ways to combat it.

Training Together

New FBI Academy Program Integrates Agents and Intelligence Analysts



Special agent and intelligence analyst trainees learn investigative skills side-by-side during the FBI's Basic Field Training Course at the FBI Academy in Quantico, Virginia. The course is a new FBI program designed to prepare trainees for collaborative work in the field.

Today's special agents and intelligence analysts graduating from the FBI Academy are beginning their first assignments fully prepared for collaborative work in the field thanks to an innovative training program launched in 2015.

Dubbed the Basic Field Training Course (BFTC), the new program offers an integrated curriculum that places new agent and intelligence analyst trainees together in a squad-like environment—the way agents and analysts work in actual FBI field offices. During the course, trainees learn skills like conducting investigations, interviewing, and providing briefings. Their academic training culminates with criminal and counterterrorism exercises modeled after real-world scenarios.

“The BFTC serves as an important element of our continued efforts to improve collaboration throughout the organization,” said Mark

Morgan, assistant director of the Bureau's Training Division. “From their first days in the FBI, special agents and intelligence analysts sit side-by-side, wear the same uniforms, and learn the necessity of working as a single, integrated, cohesive team. This is an exciting shift in the way we do things.”

Prior to launching the BFTC, agents and intelligence analysts historically trained under separate programs. While the new program integrates trainees where appropriate, specialized courses are still provided to students based on what their roles will be in the field. For example, special agents are instructed on the fundamentals of operating firearms and tactical driving, while intelligence analysts are taught how to analyze emerging threats and provide intelligence reports.

“We changed the way our students learn by integrating special agent

and intelligence analyst instructors in the classroom—the lessons are presented by a team,” said Zachary Lowe, chief of the Training Division's Instruction Section. “Having great instructors with current field experience integrating intelligence and operations has been critical to the success of the BFTC.”

The first group of graduates to complete the new training course walked across the stage at the FBI Academy this past fall to receive their credentials. One of those graduates was Alexandra, who now serves in the field as an intelligence analyst. Like other students in her class, Alexandra felt the program provided her with an invaluable experience.

“There was a great deal of cohesion within our group. We didn't see each other as agents and analysts—we were just one class,” she said. “Having this type of integrated

training, I believe, is the right step for the future of the FBI. Since we're going to be working together in the field, it only makes sense to start us off so that collaboration is the only thing we know."

The BFTC was developed in response to a key recommendation made in the 9/11 Commission Report, which called for the FBI to integrate its workforce and implement a dedicated team approach to national security operations. The curriculum of the new program answers this call by providing trainees with the necessary building blocks to further the FBI's dual law enforcement and intelligence mission.

"Students completing the course now have a broader knowledge base to help them acclimate to the workforce," said Catherine Fletcher,

chief of the Training Division's Curriculum Management Section.

Fletcher's group played an integral role in developing the program's learning components. Numerous subject matter experts as well as Headquarters and field office personnel were enlisted to provide input on the fundamental aspects of the program. Once the course's curriculum was produced, it was thoroughly reviewed to ensure the content was relevant, current, and met the needs of the FBI's mission. In all, the program was built from the ground up over the span of three years.

"During the BFTC development process, we focused on areas that would deliver the foundational skills needed for agents and analysts to understand each other's roles," said Fletcher. "By bringing

in specialists from the field, holding focus groups, and connecting to the FBI's current policies and procedures, we believe that this new curriculum achieves the end goal of instilling a team culture."

Now in its 10th month at the FBI Academy, the BFTC is providing hundreds of new agents and intelligence analysts with the tools to succeed in the field as a seamless unit. Over time, the program will continue to evolve as new investigative and intelligence-gathering techniques emerge.

"We all have a stake in this new holistic approach to training, and we'll need to stretch and learn accordingly," said Fletcher. "In the end, we're working as equal partners to support the FBI and the intelligence community as a whole."



FBI Director James Comey hands credentials to a new intelligence analyst during a Basic Field Training Course graduation last fall at the FBI Academy in Quantico, Virginia.

Tracking Animal Cruelty

FBI Collecting Data on Crimes Against Animals



Acts of cruelty against animals are now counted alongside felony crimes like arson, burglary, assault, and homicide in the FBI's expansive criminal database.

On January 1, the Bureau's National Incident-Based Reporting System (NIBRS) began collecting detailed data from participating law enforcement agencies on acts of animal cruelty, including gross neglect, torture, organized abuse, and sexual abuse. Before this year, crimes that involved animals were lumped into an "All Other Offenses" category in the FBI's Uniform Crime Reporting (UCR) Program's annual Crime in the United States report, a survey of crime data provided by about 18,000 city, county, state, tribal, and federal law enforcement agencies.

By adding animal cruelty offenses to NIBRS, law enforcement agencies and the advocacy groups that pushed for the inclusion in the FBI database are hoping the results will reveal a more complete picture of the nature of cruelty to animals.

"Some studies say that cruelty to animals is a precursor to larger crime," said Nelson Ferry, who works in the Bureau's Criminal Statistics Management Unit, which manages NIBRS. "That's one of the items that we're looking at."

The National Sheriffs' Association was a leading advocate for adding animal cruelty as a data set in

the Bureau's collection of crime statistics. The association for years has cited studies linking animal abuse and other types of crimes—most famously, murders committed by serial killers like Ted Bundy, Jeffrey Dahmer, and the "Son of Sam" killer David Berkowitz. The organization also points out the overlap animal abuse has with domestic violence and child abuse.

"If somebody is harming an animal, there is a good chance they also are hurting a human," said John Thompson, deputy executive director of the National Sheriffs' Association. "If we see patterns of animal abuse, the odds are that something else is going on."

A first look at NIBRS animal cruelty statistics will be available next year, but it will take at least three to five years for the data to begin showing helpful patterns. Groups that advocated for the new animal cruelty data hope that by adding it to NIBRS—rather than the summary-based statistics agencies provide the Bureau each year—they will get a much richer data set from which to mine. That's because NIBRS requires participating agencies to not only report crimes but also all the circumstances of a crime. Additionally, the Bureau plans to phase out summary-based UCR statistics—which have been collected roughly the same way since 1930—in favor of NIBRS by 2021.

"With summary data, all I can tell you is a crime occurred," said Amy Blasher, who is leading the broader transition to NIBRS at the FBI's Criminal Justice Information Services Division, keeper of the Bureau's various crime data stores. "With the incident-based, it's more granular. It tells the story."

The move to collect more granular data requires agencies to adjust how they track and disseminate crime statistics. Only about 31 percent of the country is represented in NIBRS today—a fraction of the overall UCR participants; however, Blasher anticipates the figure to grow larger as law enforcement agencies opt in, including police departments in Washington, D.C. and Chicago over the next two years. The FBI is aggressively pushing for the transition to NIBRS. In a speech last March in Atlanta, FBI Director James Comey said it was his personal mission to get better data "that we can all use to have informed conversations about the most important issues we face."

Those who lobbied for better animal abuse data would agree. "With this information, law enforcement and victim services would be able to better target their intervention efforts with respect to both animal cruelty and those crimes for which animal cruelty serves as a marker," said Dr. Mary Lou Randour of the Animal Welfare Institute, which worked closely with the National Sheriffs' Association to advance their cause. "Identifying and analyzing animal cruelty crimes would provide an important tool for law enforcement."

The National Sheriffs' Association's John Thompson urged people to shed the mindset that animal cruelty is a crime only against animals. "It's a crime against society," he said, urging all law enforcement agencies to participate in NIBRS. "By paying attention to [these crimes], we are benefiting all of society."

Raising Awareness of Opioid Addiction

FBI, DEA Release Documentary Aimed at Youth

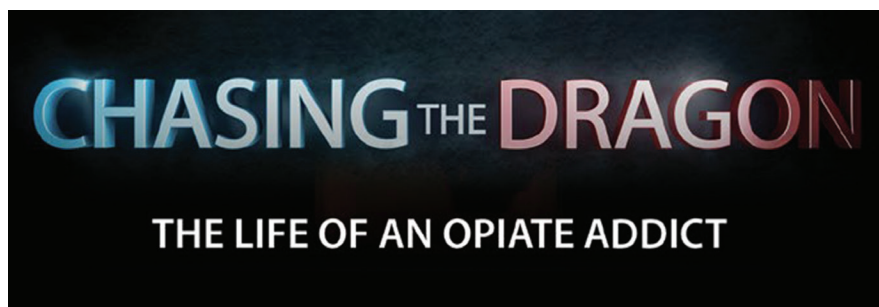
Every day, the nation's law enforcement agencies at the local, state, and federal levels—including the FBI and the Drug Enforcement Administration (DEA)—use investigative resources to target the supply side in the war against drugs.

But even with numerous law enforcement successes in this area, the demand for drugs continues. And one of the more worrisome trends is a growing epidemic of prescription opiate and heroin abuse, especially among young people.

Today, in an effort to help educate students and young adults about the dangers of opioid addiction, the FBI and DEA unveiled a documentary called *Chasing the Dragon: The Life of an Opiate Addict* at the Newseum in Washington, D.C., before an audience of educational leaders from the region. The 45-minute film, whose title refers to the never-ending pursuit of the original or ultimate high, features stark first-person accounts told by individuals who have abused opioids or whose children have abused opioids, with tragic consequences.

"This film may be difficult to watch," explains FBI Director James Comey, "but we hope it educates our students and young adults about the tragic consequences that come with abusing these drugs and that it will cause people to think twice before becoming its next victim."

And according to Acting DEA Administrator Chuck Rosenberg, "The numbers are appalling—tens of thousands of Americans will die this year from drug-related deaths, and more than half of these deaths are from heroin and prescription



In an effort to combat the growing epidemic of prescription drug and heroin abuse, the FBI and DEA have released *Chasing the Dragon: The Life of an Opiate Addict*, a documentary aimed at educating students and young adults about the dangers of addiction.

opioid overdoses. I hope this [documentary] will be a wakeup call for folks."

The individuals featured in the film—a few of whom are highlighted below—chose to tell their stories to help stop others from going down the same destructive path.

- Katrina, a former business executive and mother who became addicted to opiates after self-medicating with pain pills and alcohol and whose own daughter died of a drug overdose. "You can't go back and say, 'I'm sorry,' or set a better example, or talk 'em out of it," she says. And of her own addiction, she explains, "The spiral down is so fast...and I lost everything. I lost my daughter first and foremost. So all the work I did, all those dreams I had, it's like I'm starting over again with a huge weight on my shoulder...all for a pill."
- Matt, who began using marijuana at age 11 and became addicted to opiates at age 15. "In the beginning," he explains, "I would always try to get pills because you know what you're getting. Eventually, that just got too expensive...so then you'd go for heroin because it's cheaper."
- Trish, whose daughter Cierra—an honor roll student at her

high school—died after a heroin overdose. "Cierra did not take life for granted until she started using," says her mother. "It is much stronger than you, and it will win." Noting the broader impact of addiction, Trish adds, "It affects everyone in your family for the rest of their life...we're the ones stuck missing you."

Chasing the Dragon also features interviews with medical and law enforcement professionals discussing a variety of issues, including how quickly addiction can set in, how the increasing costs of prescription opioids can lead to the use of heroin as a less expensive alternative, the horrors of withdrawal, the ties between addiction and crime, and the fact that, contrary to popular belief, opiate abuse is prevalent in all segments of society.

The documentary is available on our website for viewing or downloading. Copies can also be obtained by contacting your local FBI or DEA field office.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/chasingthedragon.

Countering Violent Extremism

FBI Launches New Awareness Program for Teens



Don't Be a Puppet: Pull Back the Curtain on Violent Extremism is an interactive website developed by the FBI to open the eyes of teens to the devastating reality and deceptive messaging of violent extremism and to help strengthen their resistance to radicalization and possible recruitment.

Today like never before, violent extremists of all kinds are deliberately targeting our nation's young people with poisonous propaganda—especially in cyberspace, where they are flooding social media with slick recruiting videos and persuasive calls to action.

The FBI's investigations and analysis indicate that these

efforts—to a disturbing degree—are succeeding. Across America, there are young people who are embracing various forms of violent extremism, actively communicating with violent extremists, and helping with recruitment. Without warning, many teens are joining violent extremist groups in the U.S. or leaving their families and traveling to war zones thousands

of miles away to enlist in violent extremist movements—some are even plotting and launching attacks in the U.S. and overseas.

In this hyper-connected world—where violent extremist information is only a click away—it's more crucial than ever that young people learn what violent extremism really is, how it hurts innocent victims and perpetuates

Overview of the Don't Be a Puppet Website

Teens earn an FBI certificate by completing all of the activities in the five sections outlined below. Throughout the site, including during an introductory video by FBI Director James Comey, it is emphasized that free speech and religious liberty are protected under the Constitution of the United States and that having extremist beliefs is legal unless violence is directly advocated or used.

Section 1: What is Violent Extremism?

- Defines violent extremism and explores five of its key elements: blame, distorted principles, symbols, propaganda, and groupthink.
- Explains how violent extremists use their warped characteristics to manipulate, radicalize, or recruit others to embrace their ideologies.

Section 2: Why Do People Become Violent Extremists?

- Examines the key reasons why people embrace violent extremism and its ideologically motivated grievances.
- Makes teens aware of the arguments violent extremists use to justify their actions as well as highlights unmet needs and personal problems that violent extremists might exploit in their recruitment efforts.

Section 3: What are Known Violent Extremist Groups?

- Provides an overview of several violent extremist groups—typically called international terrorist organizations—and key domestic violent extremism ideologies.
- Helps teens recognize and reject these organizations and their belief systems in case they are contacted

or encounter violent propaganda on the Internet.

Section 4: How Do Violent Extremists Make Contact?

- Explores the various ways—such as social media, cell phones, and flyers—that violent extremists try to reach young people.
- Informs teens of the potential dangers of different online and offline communications channels and how these tools could be used for recruitment.

Section 5: Who Do Violent Extremists Affect?

- Features videos of survivors of violent extremism and hate crime, who share their personal stories on how they have been impacted.
- Gives teens insight into the very real pain, suffering, and losses caused by these acts of violence.

violence, and how its recruiting strategies are intended to deceive.

Today, as part of its leading role in helping to prevent terrorist attacks and in sharing its expertise on public safety issues, the FBI is taking the next step in educating communities on violent extremism by launching a new, free program for teens nationwide.

It's called Don't Be a Puppet: Pull Back the Curtain on Violent Extremism, and the centerpiece is an interactive website at <https://cve.fbi.gov> that uses activities, quizzes, videos, and other materials to teach teens how to recognize violent extremist messaging and become more resistant to self-radicalization and possible recruitment.

The site doesn't refute violent extremist beliefs point by point or discuss matters of faith or politics. Instead, it makes teens aware of the destructive reality of various forms of violent extremism, including hateful attacks based on race, religion, or other factors. Through its Don't Be a Puppet theme, the program encourages teens to think for themselves and display a healthy skepticism if they come across anyone who appears to be advocating extremist violence.

The Don't Be a Puppet initiative was developed through the combined efforts of the FBI Office of Public Affairs (OPA) and the Countering Violent Extremism (CVE) Program in the Bureau's Office of Partner Engagement, with the input and support of other FBI components. A number of community leaders, government and law enforcement officials, high school teens, and other public and private partners from across the U.S. evaluated the site and provided valuable feedback. The

Other FBI Youth Programs

From violent gangs to cyber security, the FBI has long been in the business of sharing its expertise on public safety issues with a diverse cross-section of young people through various community outreach efforts. Among the FBI's youth programs:

Adopt-a-School/Junior Special Agent Program: Puts FBI special agents and professional staff into local schools to mentor and tutor kids, showing them how to resist bad influences that could lead them to crime, drug use, gang participation, and violence. During the last fiscal year, more than 800 teens participated in these programs in 28 different FBI field offices.

Safe Online Surfing Internet Challenge: Educates third- to eighth-grade students on cyber safety and online etiquette. Since October 2012, more than 600,000 students in 49 states, the District of Columbia, and three U.S. territories have participated in the program.

Teen Academy: Gives middle and/or high school students an inside look at the FBI and fosters a greater understanding of the Bureau's work in the community. During the last fiscal year, nearly 1,400 students took part in these academies in 37 field offices.

consensus was that the program is a positive, proactive tool that addresses a serious threat.

"We want teens to apply their critical thinking skills to this issue just like they would to any subject in school," says Jonathan Cox, head of the OPA unit that created the website and developed the concept. "We're saying, 'Don't be a puppet,'—in other words, don't just blindly accept what violent extremists tell you or you could end up being controlled and manipulated by people who want you to hurt or kill innocent people."

The website is divided into five main sections, each with various activities and elements to complete (see above sidebar for more information). A sixth "Where to Get Help" page offers conflict resolution tips, identifies resources to contact for assistance, and provides links to more information. Teens receive a printable certificate upon completion of the site.

The program is open to anyone in the United States who wishes to participate, but it is designed for a teenage audience. No registration

is required to sign up for or use the website. The Bureau also recommends that community groups, resource officers, coaches, school administrators, and parents and families review the site and use it to raise awareness of violent extremism and its growing impact on our nation.

To learn more, visit the Don't Be a Puppet: Pull Back the Curtain on Violent Extremism website. Community groups, parents, and teachers who are interested in using the program can also discuss the details with the community outreach specialist in their local FBI field offices.

Incidents like the Charleston shootings and the Boston Marathon bombings have demonstrated that extremist violence transcends race and religion and can have a devastating impact on communities. It's the FBI's hope that this new initiative can make a difference in helping to keep young people from being radicalized and recruited, now and in the future.

Operation Ghost Guard

Widespread Public Corruption Inside Georgia Prisons



The FBI's Atlanta Division today announced the results of an investigation into widespread public corruption within the Georgia prison system that uncovered extensive crimes carried out by inmates with the help of corrupt guards—crimes whose impact was felt well beyond prison walls.

Nearly 50 former and current Georgia Department of Corrections officers were indicted today for accepting bribes in exchange for protecting what they believed to be drug shipments. Last month, 15 corrections officers, 19 civilians, and 19 inmates were also indicted, and a large amount of contraband—including drugs, weapons, and, in particular, cell phones—was recovered.

FBI Atlanta Special Agent in Charge J. Britt Johnson called the two-year investigation, dubbed Operation Ghost Guard, “unprecedented” in scope. “While the vast majority of those working within Georgia’s correctional

facilities are dedicated and loyal officers and employees,” Johnson said, “criminal and corrupt activities were found in 11 of the 35 state corrections facilities. Central to those illegal activities inside the

prisons was the unbridled use of cell phones.”

Today’s indictments focused on correctional officers who were willing to sell their badges—to use

Phone Scams from Prison

Georgia inmates with contraband phones and their accomplices outside of prison raised tens of thousands of dollars using various fraud schemes. Here’s how the “jury scam” worked:

- Prisoners with smartphones provided by corrupt guards accessed the Internet to identify and target potential victims from all over the country.
- Inmates called potential victims, impersonated law enforcement officials, and claimed the individuals had failed to appear for jury duty. The victims were told they had the choice of either being arrested on warrants or paying fines to have the warrants dismissed.
- To make the calls seem real, inmates created voicemail greetings on their contraband phones that identified themselves as members of legitimate law enforcement agencies. “They sounded like deputies from a sheriff’s office,” one FBI agent said. “They were very sophisticated and believable.”
- Many victims agreed to pay fines. They were instructed to purchase pre-paid cash cards and provide the account number to the inmate, or wire money directly into a pre-paid debit card account held by the inmate.
- When inmates received pre-paid cash card account numbers, they used their contraband phones to contact accomplices outside of prison who then transferred the money to a different pre-paid card, which could then be turned into cash.
- That effectively laundered the money, which could then be transferred back to the inmate.

their law enforcement credentials to protect what they believed to be drug deals involving large shipments of methamphetamine and cocaine. In a series of FBI undercover operations, more than 45 officers agreed to protect the supposed drug deals in exchange for thousands of dollars in bribes. During the undercover deals, the officers often wore their official uniforms or displayed their badges to avoid law enforcement scrutiny.

Operation Ghost Guard, undertaken in collaboration with the Georgia Department of Corrections, revealed that corrupt guards typically earned \$500 to \$1,000 for smuggling a single cell phone to a prisoner. Between 2014 and 2015, more than 23,500 contraband phones were seized throughout Georgia prisons—which house 50,000 inmates—and those phones were used for a variety of crimes that put prison security and public safety at risk.

Contraband phones were used to organize drug trafficking inside prisons and to perpetrate identity theft and phone scams that raised “tens of thousands of dollars,” said Special Agent Dan Odom. Odom supervises the FBI’s public corruption squad in Atlanta and helped coordinate the Operation Ghost Guard investigation through the FBI-led Atlanta Public Corruption Task Force, which combines the resources of numerous state and local law enforcement agencies in Georgia.

The illicit money raised through so-called “jury scams” and other frauds (see sidebar) was often used to bribe prison guards. “This was a massive investigation,” Odom said. “We identified and indicted approximately 130 subjects.” He added, “The FBI could never



U.S. Attorney for the Northern District of Georgia John Horn speaks at a press conference announcing the results of Operation Ghost Guard on February 11, 2016. He was joined by FBI Atlanta Special Agent in Charge J. Britt Johnson, Georgia Department of Corrections Commissioner Homer Bryson, and FBI Atlanta Assistant Special Agent in Charge Doug Korneski (left to right), among other officials.

have worked this case without the assistance of the Department of Corrections. They recognized they had a problem, and they wanted to fix it.”

Operation Ghost Guard began in May 2014, shortly after a kidnapping that was set in motion by a prisoner with a contraband phone. The prisoner, serving a life sentence in North Carolina, wanted revenge on the prosecutor who helped put him there.

Using that contraband phone, the prisoner enlisted the help of fellow gang members in Atlanta who were not incarcerated to kidnap the prosecutor’s father in North Carolina and drive him to Atlanta, where he was to be tortured and killed. The FBI’s Hostage Rescue Team was able to rescue the man before gang members killed him, “but the risk of life to this individual was very real,” Johnson said. “All because of a cell phone in a prison.”

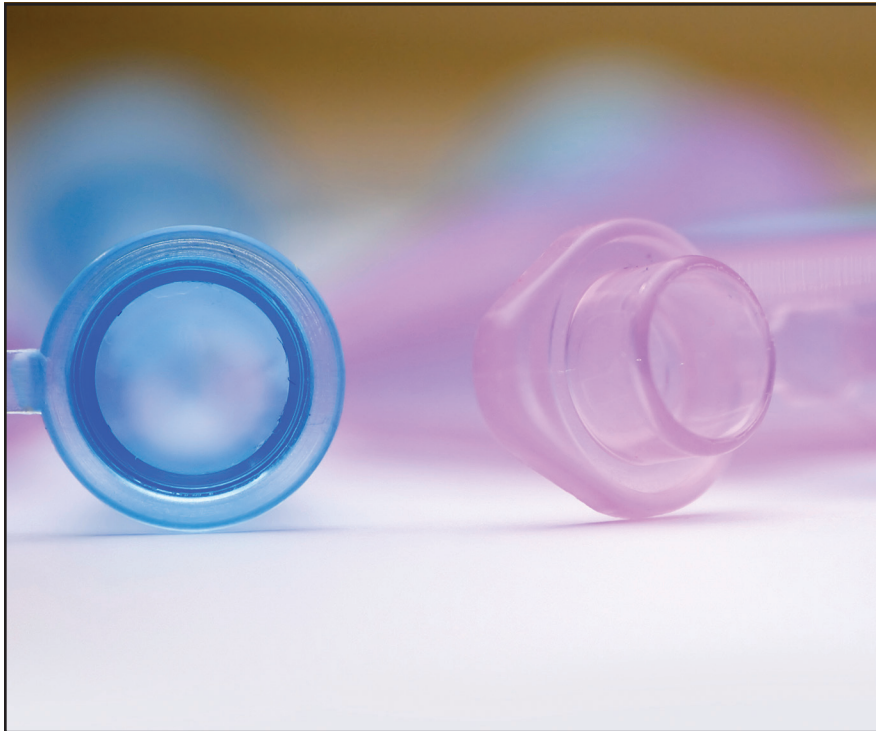
That incident served as a catalyst for Operation Ghost Guard. It also prompted the FBI’s Public Corruption Unit in Washington, D.C., to launch the nationwide Prison Corruption Initiative.

“Because of one small act of corruption—a guard giving a cell phone to an inmate—many serious crimes can occur,” said Special Agent Joe Gonzalez, who heads the Bureau’s Public Corruption Unit at FBI Headquarters. “This is not just Georgia’s problem, it’s a national problem.”

Gonzalez said that since the Prison Corruption Initiative was launched in June 2014, the number of FBI public corruption cases in prisons nationwide has tripled. “Corrections officers might not be elected officials,” he added, “but they are public officials sworn to protect the community, and we are going to hold them to that standard.”

Egg Donation and Surrogacy Scam

California Woman Robbed Would-Be Parents of Money and Hope



Allison Layton, who owned a California company called Miracles Egg Donation (Miracles), claimed she was in the business of helping infertile couples have children. But her business turned out to be a fraud, and she ended up stealing her victims' hopes and dreams as well as their money.

Would-be parents paid Miracles tens of thousands of dollars—sometimes their life savings—for egg donation and surrogacy services that Layton promised to coordinate. Instead, during a three-year period beginning in 2008, she defrauded couples, egg donors, and surrogate mothers while living a lavish lifestyle off the proceeds.

“This was not a typical white-collar case,” said Special Agent Dana Eads, who led the investigation from the FBI’s Los Angeles Division. “Many of the victims were in a vulnerable place in their lives—working against their biological clocks and trying to afford this expensive

and time-consuming procedure. Some told the judge that because of Layton’s actions, they had effectively missed the opportunity to have children.”

The fees paid to Miracles by would-be parents—known in the surrogacy world as intended parents—were supposed to go into escrow accounts to be withdrawn for expenses related to surrogacy or egg donation. But Layton took the money and spent it on her own \$60,000 wedding, a new vehicle for her husband, and high-end shopping sprees she flaunted on social media.

As a result, egg donors, surrogates, attorneys, and others often were not paid for the services they provided, and many intended parents—including some who lived overseas—failed to get the services they paid for.

“It became like a Ponzi scheme,” Eads explained. “Early on, some people got the services they paid for. But then Layton began

shuffling funds to cover some clients’ services and not others. And when it all finally collapsed, nobody was getting anything.”

When confronted by clients, Layton lied about why payments had not been made and refunds not issued. She led victims to believe they might soon be paid, when, in fact, many were not. Eventually, several victims contacted the FBI while others filed reports with the local police department in Glendora, California. Court records indicate that more than 40 victims lost in excess of \$270,000.

Layton maintained she had simply made poor business decisions, but through interviews, bank records, and e-mail correspondence, Eads soon uncovered the fraud.

“The scam was apparent, especially when we examined her bank records,” Eads said. “Layton regularly told clients their checks—which she never wrote—must have been lost in the mail. She told that to so many people. That story, told the same way again and again, was a clear indication of her attempt to hide the truth.”

In 2014, Layton was charged with wire fraud. In a pre-indictment plea agreement with federal prosecutors, she admitted defrauding the victims, and in September 2015, a judge sentenced the 38-year-old to 18 months in prison.

Considering the damage that she caused—both financial and emotional—some of Layton’s victims believe she got off too easy. Eads understands how they feel. “But as a result of this case,” she said, “Layton is now a convicted felon, and part of the plea she accepted is that she can never work in this industry again.”

Counterfeit Cabs

Auto Broker Who Used Salvage Vehicles as Taxis Sentenced

Every day in communities around the nation, the FBI works with its state and local partners to identify and arrest criminals who threaten public safety—including terrorist groups, violent gangs, drug trafficking enterprises, and producers of counterfeit pharmaceuticals, auto parts, and airplane parts.

Most recently, the FBI, in conjunction with the Inspector General for the City of Chicago, conducted an investigation into a fraud scheme that involved the illegal use of salvage vehicles as taxis on city streets—a scheme that potentially put the riding public at risk.

Last month, Chicago auto broker and taxicab operator Alexander Igolnikov was sentenced to a federal prison term after previously pleading guilty to conspiracy to transport, receive, and possess a counterfeit security—in this instance, that “security” was an illegally obtained clean vehicle title for a salvage car.

A vehicle can receive the “salvage” designation—usually from a state motor vehicle agency—for a number of reasons, including having been stolen, vandalized, in an accident, in a flood or other natural disaster, etc. And once a salvage title is issued, there’s often no legal mechanism to obtain a “clean” title for the same vehicle.

But there are illegal mechanisms, and that’s just what Igolnikov and several associates used to get rid of the salvage designation.

In his plea agreement, Igolnikov admitted to running a scheme from 2007 through April 2010 that involved buying significantly damaged vehicles with salvage titles from online auction sites. He



purchased the vehicles in the name of the business he owned—Seven Amigos Used Cars—and had the vehicles towed to the Chicago address that housed Seven Amigos and a company called Chicago Carriage Taxi. Once there, the cars were repaired.

In the meantime, several of Igolnikov’s associates worked on taking care of the salvage designations on the purchased vehicles by submitting fraudulent paperwork to the nearby Indiana Bureau of Motor Vehicles in an effort to obtain “rebuilt” titles. Under Indiana law, a vehicle that had been issued a salvage title could be repaired and issued a title with a rebuilt designation if the vehicle was examined by a law enforcement officer who certified that the vehicle had been repaired properly. Igolnikov’s associates submitted paperwork purportedly certifying that an officer had examined their vehicles and that the repairs conformed to Indiana law, but in reality, no officer ever examined their vehicles.

For Igolnikov’s scheme to work, though, the rebuilt title was not

good enough. Chicago’s city rules would not allow a vehicle with either a salvage or rebuilt title to be approved as a taxicab. So he and his associates took it one step further: They placed a sticker, usually one purporting to be from an online auction, over the “rebuilt” section of the Indiana title to conceal the fact that the title had a rebuilt certification. They then used that title to obtain a clean title from the Illinois Secretary of State’s Office. Armed with the clean title, Igolnikov could apply for a license to operate the vehicle as a taxicab in Chicago. And for approximately three years, he and his associates operated approximately 112 salvage—and potentially unsafe—taxis on Chicago streets.

But the scheme was ultimately uncovered, and as a result of the close working relationship between the FBI’s Chicago Field Office, Chicago’s Inspector General, and the U.S. Attorney’s Office for the Northern District of Illinois, the individual responsible was identified and brought to justice.

Caught in the Act

Prolific Washington State Bank Robber Sent to Prison



The masked criminal known as the Cyborg Bandit and, later, the Elephant Man Bandit was robbing Seattle-area banks at an average of more than two per month for an entire year before he was caught—in the act of robbing a bank he had already robbed.

For investigators who routinely work bank robberies, the story of 46-year-old Anthony Hathaway, sentenced last month to nearly nine years in prison, is surprising in some ways but all too familiar in others.

“In this particular case and in general, bank robbery is a crime of last resort,” said Len Carver, a detective with the Seattle Police Department and member of the FBI’s Seattle Safe Streets Task Force. “Occasionally you get a thrill seeker or a truly violent individual, but most people who rob banks are supporting an addiction of some kind—drugs or gambling—and they are desperate.”

Hathaway’s addiction was to prescription painkillers and then to heroin. According to court records, he suffered an injury and became addicted to the opiate Oxycontin. After losing his job, he turned to crime to feed his addiction, and between February 2013 and

February 2014, Hathaway admitted to 30 bank robberies. He sometimes hit the same bank multiple times.

“Seattle has had many serial bandits over the years,” Carver said, “but Hathaway was prolific. He might top the list for sheer number of robberies in a one-year period.”

During the holdups, which usually occurred late in the afternoon, Hathaway wore a mask and gloves. In the early crimes, he wore textured metallic fabric over his face and was nicknamed the Cyborg Bandit because the disguise was similar to that of cyborgs in science fiction productions. After that disguise began receiving too much media attention, he covered his head with a shirt and cut out two eye holes. That earned him the nickname the Elephant Man Bandit because of the similarity to a movie character of the same name.

In several robberies, Hathaway threatened tellers, saying he had a weapon, although no weapon was ever displayed. On February 4, 2014, after a robbery in Lynwood, Washington, surveillance video showed what might have been the robber’s getaway vehicle: a light blue minivan with a Seattle Seahawks football decal on the

Left: Serial bank robber Anthony Hathaway—seen in these surveillance images in his Cyborg Bandit (left) and Elephant Man Bandit disguises—robbed 30 Seattle-area banks in the span of a year.

back window and an unusual, after-market exterior mirror.

A bulletin with the vehicle’s description went out to area law enforcement, and an Everett Police Department officer spotted it several days later and notified investigators. “An officer on patrol was being observant,” Carver said. “It was a key moment in the investigation.”

At that point, however, the bank robber’s identity was still unknown. The vehicle was not registered to Hathaway, and several people had access to it. FBI agents began surveillance, and on February 11, 2014 they observed a man drive away in the vehicle.

The driver spent several hours circling a Seattle bank that had been previously robbed. “It seemed clear he was going to rob the bank,” Carver said, “and we had a high confidence that whoever was driving the van and about to rob that bank was going to be good for the other robberies.”

Finally, Hathaway parked and pulled a mask over his face as he entered the bank. FBI agents and task force officers were there to arrest him moments later. Hathaway was identified and later admitted to the 30 robberies. In a plea arrangement concluded last month, he was sentenced to 106 months in prison.

“We are grateful that the Safe Streets Task Force was able to close all these robberies,” Carver said. “And we are pleased that Hathaway is no longer a threat to the community.”

Putting the Brakes on Crime

Getaway Driver Sentenced to 121 Years

Sesley Williams was a ringleader and getaway driver for a string of robberies involving multiple banks and commercial establishments in Las Vegas and nearby Henderson, Nevada. Today she's in a federal prison after being sentenced last month by a U.S. district judge.

It all started on a winter afternoon in 2012. While Williams sat in her car outside an outlet mall clothing store in Las Vegas, her accomplice, Anthony Jordan, was inside checking out merchandise. Jordan already had a sweater and a bottle of cologne in his possession when he asked an employee to bring out two watches from a locked glass container.

With the items in hand, Jordan made his way to the registers to check out. As the cashier began ringing him up, Jordan brandished a semi-automatic handgun and demanded everything from the drawer.

In all, Jordan walked out of the store with hundreds of dollars worth of stolen merchandise and cash. He found Williams waiting in the car nearby, and the two fled the scene.

Following the successful outlet store heist, Williams and Jordan continued to carry out a flurry of robberies between December 2012 and March 2013. In a span of just a few short months, Williams, Jordan, and a third accomplice led an intense crime spree, lifting merchandise and emptying cash registers at businesses and banks in the region.

Anything from clothing stores and fast food chains to banks inside grocery stores were consistently targeted by Williams and her group. Although she never stepped inside the businesses that were



Sesley Williams used this white Chevrolet Cavalier as one of her getaway vehicles for multiple robberies in Las Vegas and nearby Henderson, Nevada.

robbed, Williams supplied disguises and a handgun while fulfilling the role as getaway driver for every crime.

The unprecedented number of robberies committed by the group left frightened store employees and empty cash registers in their wake. But the spree ended after a tip made to the FBI's Las Vegas office spurred the Bureau's Las Vegas Criminal Apprehension Team and Safe Streets Gang Task Force to action. The task force combines FBI special agents with detectives from the Las Vegas Metro Police Department and Henderson Police Department to pool expertise in targeting violent criminals, fugitives, and gangs in the region. Williams and crew were now in their crosshairs.

Agents from the FBI's Las Vegas Field Office reviewed hours of surveillance video, conducted interviews, and used other investigative techniques that ultimately led to the arrest of Williams and Jordan in June 2013.

Following the joint investigation, a weeklong trial, and 18 convictions on 18 counts, Williams was

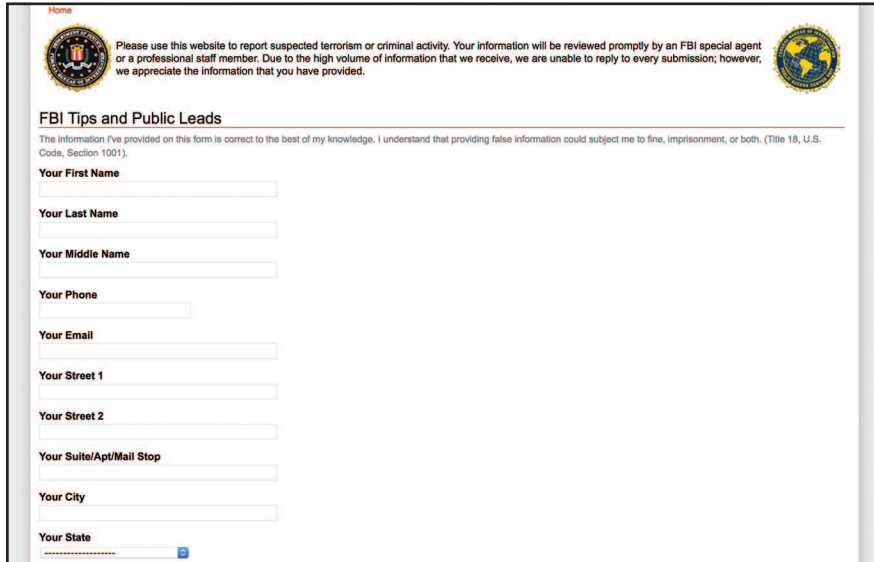
sentenced to 121 years in a federal prison for supplying a handgun and assisting as getaway driver during the rash of robberies. Jordan was dealt a similar fate after his trial and is now serving 60 years for his involvement in the crimes.

"Merely displaying a weapon during a robbery carries significant prison time—that's exactly what Williams and her crew did during these robberies," said the FBI Las Vegas agent who led the investigation. "A federal offense like this for a single robbery will land you a lengthy prison sentence. The fact that Williams was convicted of five counts of brandishing a firearm during the robberies puts her in jail for a lifetime."

While Williams' getaway-driving days are over, the FBI continues to apprehend dangerous criminals like her and Jordan by coordinating with local, state, and federal law enforcement agencies and citizens in the community. Solving violent crimes in cities like Las Vegas is also made possible through public leads and tips submitted on tips.fbi.gov.

FBI Tip Line

Web Portal Receives 'Actionable' Tips Daily

A screenshot of the FBI's online tip submission form. At the top, there is a header with the FBI seal on the left and a globe icon on the right. The text in the header reads: "Please use this website to report suspected terrorism or criminal activity. Your information will be reviewed promptly by an FBI special agent or a professional staff member. Due to the high volume of information that we receive, we are unable to reply to every submission; however, we appreciate the information that you have provided." Below this is the title "FBI Tips and Public Leads" and a disclaimer: "The information I've provided on this form is correct to the best of my knowledge. I understand that providing false information could subject me to fine, imprisonment, or both. (Title 18, U.S. Code, Section 1001)." The form contains several input fields: "Your First Name", "Your Last Name", "Your Middle Name", "Your Phone", "Your Email", "Your Street 1", "Your Street 2", "Your Suite/Apt/Mail Stop", "Your City", and "Your State". Each field has a corresponding label and a small blue icon next to the "Your State" field.

In the pre-dawn hours of October 22, 2014, a New Hampshire man was browsing a popular Internet message board when he came across what appeared to be an anonymous threat: "I'm going to shoot up University of Louisville's Miller hall [sic] tomorrow at 10 a.m."

The man went to the FBI website and submitted a tip at 4:23 a.m. Eastern Time. "Some idiot is making threats," he wrote on tips.fbi.gov, and included a link to the suspicious post. Within a minute, an FBI agent in the unit that administers the FBI's global tip line picked up the tip, setting in motion a process that happens on average 1,300 times a day. Several analysts assessed the tip and deemed it credible. The unit's supervisory special agent immediately called the university's campus police as well as local police. They were on the scene by 8 o'clock that morning and quickly arrested an 18-year-old student suspected of posting the threat.

The case illustrates how a tip—no matter how cryptic, innocuous, or far-fetched the information may seem—can help prevent violent acts. Tips to the FBI have led to

captures of Top Ten fugitives and short-circuited scores of criminal and terrorist plots. Established in 2001 in the wake of the 9/11 terrorist attacks, the tip line receives about 100 "actionable" tips every day related to possible criminal, cyber, terrorism, and espionage acts. Since its inception, the public has submitted more than four million tips via the Internet at tips.fbi.gov. In addition, phone calls to FBI field offices result in thousands of pieces of reporting a day.

"We don't want to wait for an incident. The whole push is for us to identify the next shooter or the next bomber who goes from troubled thoughts to evil deeds."

"We will check them all," said William Dayhoff, head of the tips unit, which is staffed around the clock by about two-dozen Bureau employees. In most cases, after tips are assessed they are routed to FBI field offices and local law enforcement agencies for follow-up.

Intensified efforts by foreign

Left: The FBI's global tip line, at tips.fbi.gov, was established in 2001 after the 9/11 terrorist attacks.

extremist groups to radicalize individuals in the U.S.—and recent arrests of individuals apparently heeding their call—raise the necessity for the public to send tips or contact their local field office when something looks awry.

"We don't want to wait for an incident," said Jane Rhodes-Wolfe, of the FBI's Counterterrorism Division. "The whole push is for us to identify the next shooter or the next bomber who goes from troubled thoughts to evil deeds."

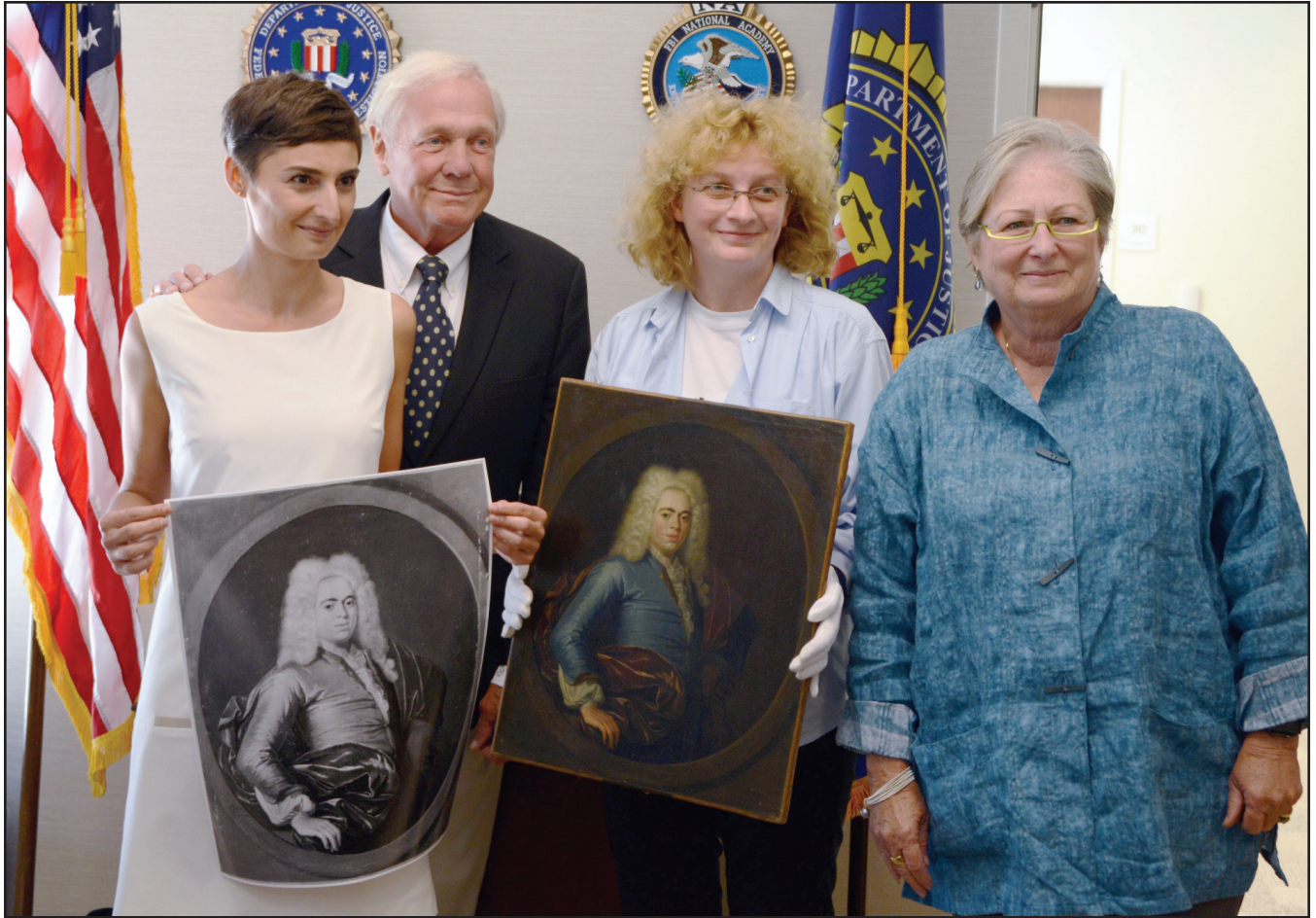
Dayhoff said the public shouldn't worry about whether a tip contains good or bad information. The most helpful tips, however, contain context—the more information, the better. Sometimes it's like a mosaic, with different pieces coming from different places. In the case of the Louisville school threat, the tip was submitted by an individual nearly 1,000 miles away. In the 48 hours after the Boston Marathon bombing in 2013, more than 50,000 tips were submitted to the FBI, half of those through tips.fbi.gov. "It's our job to put the pieces together," Dayhoff said.

Some of the most valuable tips come from people closest to subjects—people who can see changes in mood and habits and can make a common-sense assessment that things aren't right.

Rhodes-Wolfe said she understands that it can be a very hard decision for someone to contact the FBI. "We don't take that lightly," she said. "But this is a way you can help family members or friends, and potentially save lives."

A Wartime Loss Found

FBI Assists Polish Government in Recovering Painting Lost During WWII



Following an FBI investigation in which they discovered a painting they purchased was allegedly looted by Nazi soldiers during WWII, Janis Bobb (right) and John Bobb returned Krzysztof Lubieniecki's *Portrait of a Young Man* to Polish officials during a repatriation ceremony at the FBI's office in Columbus, Ohio in September 2015.

In July 2015, when Special Agent Paul Zukas began his first day on the job at the FBI legal attaché office in Warsaw, Poland, little did he know his initial case would involve helping the country's Ministry of Culture and National Heritage recover a treasured painting allegedly looted by Nazi soldiers during World War II.

Zukas' deep appreciation for art, history, and culture would be his guide during the Bureau's two-month investigation, which ultimately led him to an Ohio couple who had purchased the painting in question—unaware that it may have been looted.

"I was two days into my assignment in Warsaw when the case was

handed to me," said Zukas. "I was beyond excited. When that case came to me, I knew was going to crack it. I was determined to find the painting and get it back where it belonged."

Poland's National Museum in Warsaw had been home to Polish baroque painter Krzysztof Lubieniecki's *Portrait of a Young Man*, completed around 1728. The painting—along with other artwork—purportedly had been taken by the Nazis circa 1944 and placed inside a palace in Austria before seemingly disappearing.

A possible clue about the missing painting surfaced in August 2009, when Bob Wittmann was leafing through an old stack of family

photographs at his home in Detroit.

Wittmann had been conducting research on his late father's World War II service record when he came across a picture taken in 1945 of then 19-year-old Private John Wittmann in full service dress. The soldier was posing in uniform in his Columbus, Ohio home alongside a number of wartime mementos he collected during his time abroad.

The photograph showed an old painting that Bob Wittmann recognized from childhood depicting a young man wearing a light blue coat and powdered wig. Wittmann also found a second photograph of the painting, which featured an inventory number and a phrase in a foreign language



An inventory label from Poland's National Museum on the back of *Portrait of a Young Man* provided a clue about the painting's rightful owner.

he didn't understand. Intrigued, he searched for the phrase on the Internet and landed on the website of the National Museum in Warsaw. Wittmann later discovered a painting that looked like the one his father brought home from the war had been reported missing by the Polish government.

"There on the Polish Embassy's Wartime Losses web page was a picture of the painting," said Wittmann. "The chills really kicked in when I saw the photograph on their website."

He eventually notified Poland's Ministry of Culture and National Heritage about the missing painting and agreed to assist them in tracking it down, thinking it could still be in his family's possession.

Wittmann's search ended after he learned a relative in Florida sold the portrait through a third party to an Ohio art collector with the last name Bobb around 1990. The Polish government then turned to the FBI for help, and that's where Zukas came in.

After poring over his newly assigned case file, Zukas learned about Wittmann through all the correspondence he already had with the Polish government. "I

knew about all the key players based on Bob Wittmann's extensive research and simply had to put the pieces together," he said.

Zukas picked up the phone and called John Bobb, the possible owner of the painting. Following their discussion, Bobb realized that the painting the FBI was searching for could be the same one hanging on his dining room wall in Westerville, Ohio. In August 2015, Bobb e-mailed a photograph of the painting to Zukas, who knew instantly it was a match.

But was the painting authentic?

That September, Bobb and his wife, Janis, brought the portrait to the FBI's Columbus Resident Agency—a satellite of the Cincinnati Field Office—where they met with a member of the Bureau's Art Crime Team and officials from the Polish government. After a series of careful examinations, it was

confirmed the painting in John and Janis Bobb's possession was indeed *Portrait of a Young Man*.

"Our minds were made up and we had already said goodbye to the painting before going to the FBI office," said Janis Bobb. "For us, it was a no brainer. We knew it should go back to Warsaw."

Although the Bobbs had to bid farewell to the painting, the FBI invited them and Polish government officials to attend a rededication ceremony at the National Museum in Warsaw last fall. There they were joined by Wittmann and his wife, as well as Zukas, to witness *Portrait of a Young Man* officially returned to its rightful place.

"Seeing the painting unveiled and back at the museum was an incredible feeling. It was the single best moment in my FBI career," said Zukas.



An art expert from the Polish government authenticates *Portrait of a Young Man* against a copy at the FBI's office in Columbus, Ohio.

Lottery Fraud

Scammers Target the Elderly

The telephone call came from out of the blue. The man on the line told the 83-year-old retired schoolteacher she had won a substantial lottery prize. All that was required to claim the windfall was to pay taxes and other fees.

Before it was over, the victim—a Virginia resident who had meticulously saved for her retirement—was out more than \$500,000 in a scam that has become all too familiar among the elderly.

The criminals behind these lottery frauds and other telemarketing scams prey on senior citizens for a variety of reasons, according to Special Agent John Gardner, who investigated the woman's case out of the FBI's Washington Field Office and eventually helped put the Jamaican man who victimized her behind bars.

"The first thing to know is that lottery scammers have no empathy for the elderly," Gardner said. "For them, it's all about the money." Seniors can be lured into the scam because they have financial difficulties, or they might have enough for themselves but want to leave a legacy for their children. Some may be suffering from mental decline or dementia. "Others are so lonely, they just want someone to talk to," Gardner explained. "Some scammers become 'best friends' with their victims."

There is also the issue of technology. The criminals—many who carry out their crimes from Jamaica—use Internet tools to mask their calls so they appear to be coming from U.S. numbers with particular area codes, such as Las Vegas.

"Elderly people grew up at a time when people weren't defrauding

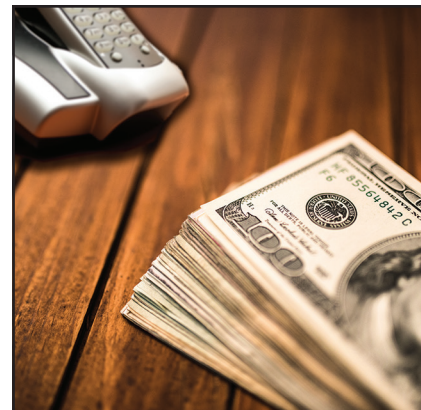
people over the phone," Gardner said. "They are not aware of these Internet masking technologies and are generally not suspicious when the telephone rings."

The fraudsters are as persuasive as they are sophisticated. "The Jamaican lottery scammers are like an organized cyber crime group," Gardner said. "They are closely knit, highly structured, and have U.S. associates—money mules—who help launder their money."

The scammers who make the calls speak excellent English and use well-practiced scripts complete with rebuttals. They are experienced and extremely manipulative. To target victims of a certain age, they buy lead lists that are widely available online.

Gardner received the Virginia woman's complaint in 2011. The ensuing investigation eventually resulted in the identification of seven subjects, all of whom were charged in connection with the lottery scheme. Six of those individuals have been convicted, and one is a fugitive. The ringleader, Paul Laing, 31, of Sandy Bay, Jamaica, was sentenced last month to 10 years in prison for his leadership role in the scheme.

Laing pled guilty in October 2015, admitting that he defrauded numerous elderly victims, including the woman from Virginia who lost her life savings. Laing instructed victims to send funds through wire transfers, the U.S. mail, and other means directly to him in Jamaica or to co-conspirators in the U.S. Those co-conspirators—the money mules—kept a portion of the proceeds and transferred the rest to Laing. The illicit funds ran to hundreds of thousands of dollars from more than 23 known victims,



Don't Fall Victim to Lottery Scams

The Federal Trade Commission—the nation's consumer protection agency—offers the following advice to avoid falling victim to lottery scams and other telemarketing frauds:

- Don't pay money to collect supposed lottery or sweepstakes winnings. If you have to pay to collect, you are not winning, you are buying. Legitimate sweepstakes don't require you to pay insurance, taxes, or shipping and handling fees to collect your prize.
- Scammers pressure people to wire money through commercial money transfer companies because wiring money is the same as sending cash. When the money's been sent, there's very little chance of recovery. Likewise, resist any push to send a check or money order by overnight delivery or courier. Con artists recommend these services so they can get their hands on your money before you realize you've been cheated.
- Remember that phone numbers can deceive. Internet technology allows scammers to disguise their area code so it looks like they're calling from your local area, but they could be calling from anywhere in the world.

Gardner said, adding that there were likely many more victims who never came forward.

Arkansas Drug Trafficking Enterprise Dismantled

Leader Gets 20 Years in Prison After Multi-Agency Investigation



Several years ago, in the city of West Memphis in eastern Arkansas, violent street gangs involved in drug trafficking and other crimes threatened the safety and security of the people who lived and worked in the area. One of the most significant gangs was headed by drug kingpin Rafael McDaniel.

After a request for federal assistance from the West Memphis Police Department to help address the drug trafficking activity and its accompanying violence, the FBI initiated Operation Delta Crossroads as an Organized Crime Drug Enforcement Task Force (OCDETF) case. And as a result of the investigation—which involved multiple controlled drug buys and several Title III wiretaps that recorded hundreds incriminating conversations—McDaniel was convicted of drug and firearms offenses last year and subsequently sentenced to a 20-year prison term. Several of his co-conspirators were also charged, pled guilty, and sentenced.

The OCDETF program, established in 1982, is the centerpiece of the Department of Justice's drug strategy to reduce the availability of drugs by identifying, disrupting, and dismantling major drug trafficking organizations and related criminal enterprises. OCDETF investigations succeed because they leverage the strengths,

resources, and expertise of federal, state, and local investigators and prosecutors.

During the investigation into McDaniel's gang, agents from our Little Rock Field Office worked side-by-side with several narcotics detectives from the West Memphis Police Department. With the assistance of the Arkansas State Police—and in coordination with the U.S. Attorney's Office for the Eastern District of Arkansas—investigators identified and gathered evidence on McDaniel's West Memphis-based drug trafficking organization, which was believed to be responsible for the distribution of large quantities of cocaine and crack cocaine in Crittenden County and other areas of eastern Arkansas.

We knew that McDaniel had two lieutenants—Wendell Glenn and David Green—who helped him run the operation. We knew that the organization regularly obtained multi-ounce quantities of cocaine from suppliers. We knew that McDaniel, Glenn, Green, and others actually converted the cocaine into crack cocaine before giving it to other organization members responsible for the sale of the drugs. And we knew that members of the criminal enterprise, including McDaniel, possessed and used firearms for the purpose of protecting their drugs and drug proceeds and to intimidate and deter rival drug dealers.

The Little Rock FBI case agent recalled an instance of overhearing talk on a wiretap between Wendell Glenn and a criminal associate who was physically tailing a rival drug dealer. The associate offered to shoot the dealer, but Glenn said

he wanted to do it himself. "But," said the agent, "the shooting didn't happen because we sent marked units to flood the area."

A July 2014 superseding indictment charged McDaniel, Glenn, Green, and 15 other conspirators with various drug trafficking and firearms offenses. Sixteen defendants, including Glenn and Green, eventually entered guilty pleas and were sentenced in the face of such overwhelming evidence (charges against a 17th defendant were combined with another federal indictment). But McDaniel, perhaps thinking he was smart enough to beat the system, took a chance on a trial—and lost.

Law enforcement collaboration in eastern Arkansas is nothing new—in February 2015, the leader of another drug trafficking organization was sentenced to life in prison after the successful conclusion of another OCDETF case, Operation Delta Blues, which targeted public corruption, drug trafficking, and unlawful firearms. And in August 2015, 70 defendants were charged with drug and gun offenses in 40 separate indictments as part of an OCDETF case known as Operation Blynd Justus.

According to the Delta Crossroads case agent, "The task force made the case. It would not have happened without both agencies [West Memphis Police Department and FBI] working closely together."

And today, communities in eastern Arkansas are enjoying dramatic decreases in violent crimes being committed on their streets as a result of these kinds of law enforcement collaborations.

Food Stamp Fraud

Supermarket Owner Imprisoned for Multi-Million-Dollar Scam

Tessema Lulseged owned a supermarket in Decatur, Georgia, but he was selling much more than groceries. He was trafficking in food stamps, and, for a time, it made him a wealthy man.

Lulseged owned the Big T Supermarket, a convenience store just outside Atlanta. He routinely and illegally allowed his customers to exchange food stamp benefits for cash—taking a substantial cut for himself. From 2009 until 2014, Lulseged’s crimes netted him approximately \$6.5 million.

“He didn’t even have to know you to trade food stamps for cash,” said Special Agent Will Filson, who investigated the case out of the FBI’s Atlanta Division along with agents from the U.S. Department of Agriculture’s Office of Inspector General.

The federal food stamp program, administered by the Department of Agriculture and supported by taxpayer dollars, is intended to offer low-income citizens nutritional assistance. Recipients are issued debit cards pre-loaded with monthly benefits that range from hundreds to thousands of dollars depending on the number of dependents in a household. Stores that participate in the program are prohibited from exchanging cash for food stamp benefits or accepting benefits for alcohol, tobacco, or other non-food items.

Lulseged allowed customers to exchange benefits for cash if they purchased groceries valued at 10 percent of the amount of cash they wanted. For example, if a customer wanted \$200 in cash, he or she was required to buy \$20 worth of groceries. The person would then get their money, and Lulseged would pocket \$150 for himself. A



total of \$350 would be deducted from the food stamp debit card.

“If you were shopping at a big-box grocery store and spent \$800,” Filson said, “you would be pushing five big carts out to the parking lot. At the Big T Supermarket, people allegedly spent that amount and were walking out with their items in a single plastic bag.”

The investigation began in 2013. Sources and undercover operatives were used to make controlled exchanges, and investigators also compared the amounts of products Lulseged bought from vendors with the amounts redeemed using food stamp benefits.

“When we compared actual vendor purchases against submitted food stamp redemption amounts, it was outrageous,” Filson said. “It was something like \$500,000 worth of products purchased and \$8 million reported in food stamp redemptions. The figures were completely skewed.”

Search and seizure warrants were executed against Lulseged in 2014, and more than \$700,000 was recovered from his various bank accounts. The government also seized Lulseged’s supermarket building and his personal residence. In 2015, Lulseged pled guilty to trafficking in food stamps. Last

month, a federal judge sentenced the 49-year-old to four years and three months in prison.

Filson praised the partnership between the FBI and the Department of Agriculture investigators. “This case was a big success not only because of the prison term but also because of the nearly \$1.5 million in cash and property forfeited to the government,” he said.

As for the food stamp recipients who illegally received cash back, Filson said the individual amounts were not substantial enough for state or federal charges to be filed. But the food stamp program has an administrative process, and those who abuse the system are subject to having their benefits suspended.

“Food stamp fraud can be a significant drain on the federal budget,” Filson said. “This \$6.5 million case was just one store. If you add up all the fraud across the country, it would likely run into the hundreds of millions.”

Case in point: Earlier this month, another Atlanta convenience store owner pled guilty to eight counts of wire fraud for illegally exchanging food stamp benefits for cash over a nearly five-year period. The scheme allegedly netted the man nearly \$2 million.

Check-Cashing Scheme Voided

Multi-Agency Effort Disrupts U.S. Treasury Check-Cashing and Identity Theft Ring



The treasury checks were meant for military families, taxpayers receiving refunds, and Social Security beneficiaries—but they wound up in the hands of thieves instead.

From June 2012 to September 2014, a band of 19 criminals in Atlanta ran a large-scale U.S. Treasury check-cashing and identity theft ring that defrauded the federal government and retail stores of nearly \$1 million. The ring included check suppliers, sellers, identification manufacturers, and “check runners” who used fake driver’s licenses to cash stolen checks.

At the center of it all was career criminal Asad Abdullah, who orchestrated the elaborate scheme from inside a Georgia state prison. With regular access to contraband cellphones, Abdullah was able to contact his younger brothers in Atlanta, and he soon had the resources he needed to mobilize the family-run criminal enterprise.

Here’s how it worked: Thieves stole checks from various sources, including the U.S. mail, and middlemen purchased the checks at a percentage of their face value,

usually 25 percent. Meanwhile, identification manufacturers were paid to produce counterfeit Georgia driver’s licenses matching the names and addresses of the victims, but with photos of the scheme’s check runners, who would cash the checks at grocery stores, discount supermarkets, and check-cashing outlets.

While U.S. Treasury check-cashing was a regular activity for Abdullah’s crew, the ambitious enterprise also engaged in credit card fraud. Inside sources working at big-box stores with regular access to customer and store credit card data provided the thieves with a steady flow of personal information. This data was used to produce counterfeit identification documents so the fraudsters could pose as real store club members. Trips to stores throughout Georgia, Tennessee, and Alabama resulted in brand new replacement credit cards that were ultimately used to purchase gift cards, gas, groceries, and other items.

The ring was finally derailed following a series of early morning raids and takedowns on September 24, 2014, which turned up weapons,

cash, and identity document manufacturing hardware.

“The 16-month investigation was an enormous cooperative effort involving numerous federal, state, and local law enforcement resources,” said an FBI Atlanta agent assigned to the case.

As part of the investigation, a confidential informant assisted the FBI and other law enforcement personnel in recovering stolen checks and false identifications. Several stores also agreed to support the investigation by cashing the stolen checks, thus aiding the Bureau and other agencies in identifying members of the scheme.

“Fraud and identity theft crimes are a serious problem in Atlanta,” added the case agent. “Our combined efforts in this particular case serve as a warning to would-be criminals on the brink of preying on unsuspecting victims.”

Sentencing was announced on February 16, 2016 for 18 of the 19 Atlanta criminals convicted for their roles in the crime ring. The 19th and final defendant is scheduled to be sentenced in the near future.

Syrian Cyber Hackers Charged

Two From 'Syrian Electronic Army' Added to Cyber's Most Wanted

Three members of a Syrian hacker collective that hijacked the websites and social media platforms of prominent U.S. media organizations and the U.S. military were charged today in federal court with multiple conspiracies related to computer hacking.

In two criminal complaints unsealed in the Eastern District of Virginia, Amad Umar Agha, Firas Dardar, and Peter Romar were charged with criminal conspiracies related to their roles targeting Internet sites—in the U.S. and abroad—on behalf of the Syrian Electronic Army (SEA), a group of hackers that supports the regime of Syrian President Bashar al-Assad. The affected sites—which included computer systems in the Executive Office of the President in 2011 and a U.S. Marine Corps recruitment website in 2013—were deemed by SEA to be antagonistic toward the Syrian government.

According to the charges, Agha, 22, known online as “The Pro,” and Dardar, 27, engaged in a multi-year conspiracy that began in 2011 to collect usernames and passwords that gave them the ability to deface websites, redirect domains to sites controlled by the conspirators, steal e-mail, and hijack social media accounts. To obtain the login information they used a technique called “spear-phishing,” where they tricked people who had privileged access to their organizations’ websites and social media channels into volunteering sensitive information by posing as a legitimate entity.

The FBI today added Agha and Dardar—both believed to be in Syria—to its Cyber’s Most Wanted. The Bureau is offering a reward of up to \$100,000 each for information that leads to their



Amad Umar Agha (left) and Firas Dardar were charged in federal court with multiple conspiracies related to computer hacking.

arrest; anyone with information is asked to contact the FBI or the nearest U.S. Embassy or consulate. Tips can also be submitted online at tips.fbi.gov.

Dardar, known online as “The Shadow,” also worked with Peter “Pierre” Romar, 36, on a scheme beginning in 2013 to extort U.S. businesses for profit. According to the complaint, the pair would hack into the victims’ computers and then threaten to damage computers, and delete or sell the data unless they were paid a ransom.

Other examples of the conspirators’ hacks include:

- Compromising the Twitter account of a prominent U.S. media organization in 2013 and releasing a tweet claiming that a bomb had exploded at the White House and injured the President.
- Gaining control of a U.S. Marine Corps recruiting website and posting a message urging Marines to “Refuse [their] orders.”

In a statement, Assistant Attorney General for National Security John Carlin said the conspirators’ extortion schemes undermine their own claims of working for a noble cause—to support the embattled regime of their president. “While some of the activity sought to harm the economic and national

security of the United States in the name of Syria, these detailed allegations reveal that the members also used extortion to try to line their own pockets at the expense of law-abiding people all over the world,” Carlin said.

The U.S. District Court has issued arrest warrants for all three defendants. The FBI’s Washington Field Office (WFO) is investigating the case with assistance from the NASA Office of the Inspector General and Department of State Bureau of Diplomatic Security, and other law enforcement agencies.

“These three members of the Syrian Electronic Army targeted and compromised computer systems in order to provide support to the Assad regime as well as for their own personal monetary gain through extortion,” said WFO Assistant Director in Charge Paul M. Abbate. “As a result of a thorough cyber investigation, FBI agents and analysts identified the perpetrators and now continue to work with our domestic and international partners to ensure these individuals face justice in the United States.”

Note: These cases may have been resolved since this information was posted on our website. Please check www.fbi.gov/wanted for up-to-date information.

International Cyber Crime

Iranians Charged with Hacking U.S. Financial Sector

WANTED BY THE FBI

CONSPIRACY TO COMMIT COMPUTER INTRUSION



Ahmad Fathi



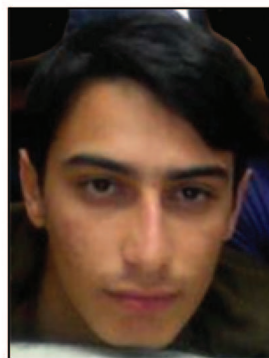
Hamid Firoozi



Amin Shokohi



Mohammad Sadegh
Ahmadzadegan



Omid Ghaffarinia



Sina Keissar



Nader Saedi

Seven Iranians working on behalf of the Iranian government have been indicted for a series of cyber crimes that cost U.S. financial institutions tens of millions of dollars and compromised critical controls of a New York dam.

Using botnets and other malicious computer code, the individuals—employed by two Iran-based computer companies sponsored and directed by the Iranian government—engaged in a systematic campaign of distributed denial of service (DDoS) attacks against nearly 50 institutions in the U.S. financial sector between late 2011 and mid-2013. The repeated, coordinated attacks disabled bank

websites and prevented customers from accessing their online accounts.

The indictments were unsealed today in federal court in New York City. The defendants are all believed to be in Iran, but Interpol Red Notices have been issued for their arrests and extraditions to the U.S. if they travel outside of Iran.

“The FBI will find those behind cyber intrusions and hold them accountable, wherever they are, and whoever they are,” said Director James B. Comey at a press conference today at the Department of Justice in Washington, D.C., where the charges were announced. Attorney

General Loretta Lynch added, “We will continue to pursue national security cyber threats through the use of all available tools, including public criminal charges.”

The DDoS attacks, which overwhelmed servers and thereby denied Internet access to legitimate users, collectively required tens of millions of dollars to mitigate. The attacks began in December 2011, and by September 2012 were occurring on nearly a weekly basis. On certain days, hundreds of thousands of customers were cut off from online access to their bank accounts.

According to court documents, one of the hackers who helped build the



Attorney General Loretta Lynch—joined by (from left) Assistant Attorney General for National Security John Carlin, FBI Director James Comey, and U.S. Attorney Preet Bharara of the Southern District of New York—announces indictments against seven Iranian hackers for cyber crimes against the U.S. financial sector at a press conference on March 24, 2016 at the Department of Justice in Washington, D.C.

botnet used in some of the attacks received credit for his computer intrusion work from the Iranian government toward completion of his mandatory military service requirement. Other defendants have claimed responsibility for hacking servers belonging to NASA and for intrusions into thousands of other servers in the U.S., the United Kingdom, and Israel.

Since the attacks, the FBI and the Department of Justice have worked with the private sector to neutralize and remediate the botnets. The Bureau also conducted extensive outreach to Internet service providers to assist in removing the malware from affected servers. Through these efforts, more than 90 percent of the threat has been successfully eliminated.

“By calling out the individuals and nations who use cyber attacks to threaten American enterprise, as we have done in this indictment, we will change behavior,” Comey said. Referring to the fact that the defendants are currently out of U.S. reach, he added, “The world is small, and our memories are long. No matter where hackers are in the world and no matter how hard they try to conceal their identities, we will find ways to pierce that shield and identify them. That is the message of this case.”

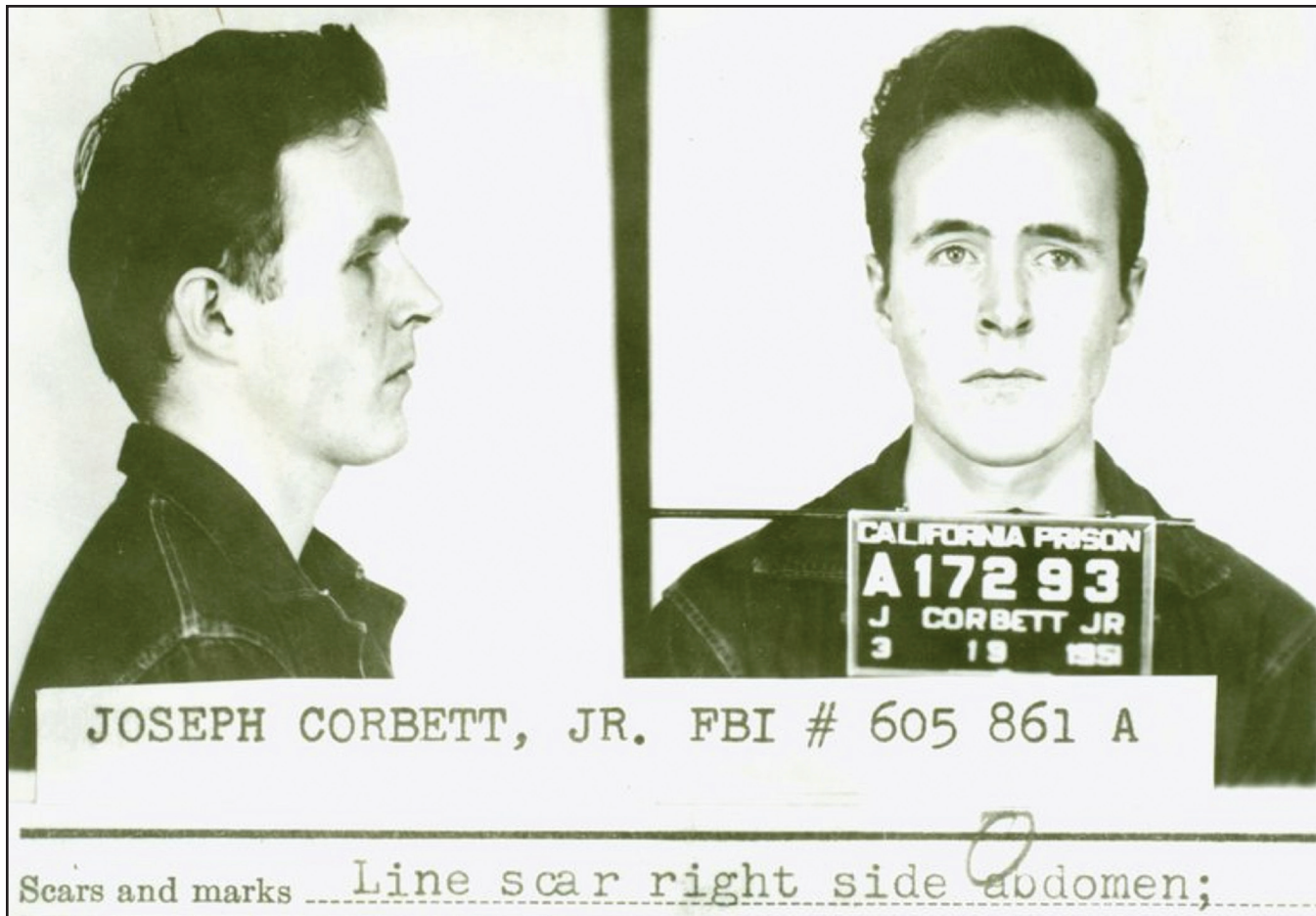
In addition to targeting the U.S. financial sector, one of the defendants repeatedly gained access to computer systems of the Bowman Dam in Rye, New York in 2013. Although the defendant never gained control of the dam, his access allowed him to learn critical information about the dam’s

operation, including details about gates that control water levels and flow rates. The breach underscored the potential vulnerabilities of the nation’s critical infrastructure to foreign hackers and could have posed “a clear and present danger to the public health and safety of Americans,” said Attorney General Lynch.

Note: These cases may have been resolved since this information was posted on our website. Please check www.fbi.gov/wanted for up-to-date information.

A Look Back at the Coors Kidnapping Case

Law Enforcement Collaboration and Public Assistance Played Key Role



This March 19, 1951 mug shot was taken upon Joseph Corbett, Jr.'s incarceration at the California Institution for Men in Chino, California, where he was sentenced to five years after pleading guilty to second-degree murder. He escaped from prison and committed the kidnapping and murder of Adolph Coors, III while a fugitive.

On February 9, 1960, a milkman sounded his horn several times in an attempt to get the attention of the driver of a station wagon that was blocking the middle of the bridge over Turkey Creek, near Morrison, Colorado. When there was no response, he got out of his truck and walked to the vehicle—it was empty, but its engine was running and the radio playing. A few more beeps on the horn didn't bring the driver back, so the milkman moved the car himself to the side of the road, noticing a reddish-brown stain on the bridge and a hat on the edge of the river bank below.

The milkman reported the matter to the local police, who quickly determined that the car belonged

to Adolph Coors, III. Heir to the Coors Brewing Company fortune, Coors had left his house—not far from the bridge—that morning, but had not been seen since. Searchers soon spread out over the area looking for the missing 45-year-old father of four. In addition to the hat, a few objects belonging Coors were found below the bridge, but no other trace was found during the wider search.

Twenty-four hours later, the FBI's Denver Division entered the case to help Colorado authorities—with the passage of a day since Coors' disappearance, the federal kidnapping statute could be invoked and the full investigative resources of the Bureau could be called upon. Coors' wife, Mary,

received a typewritten note that day demanding a ransom for the return of her husband. Under the guidance of law enforcement, she followed the instructions regarding contacting the kidnapper but heard nothing back.

The FBI Laboratory began analyzing the available evidence, especially the ransom note, which had a distinct typeface and was written on paper with an uncommon watermark.

Meanwhile, state and local police pursued leads closer to the scene of the crime, conducting extensive interviews and other investigative activities. They soon focused on a canary yellow Mercury that had been seen in the area on several

occasions and tried to track down its driver, a man who called himself Walter Osborne. The FBI learned that Osborne had disappeared around the time of Coors' abduction, but before doing so had obtained a gun, handcuffs, and a typewriter. And the Bureau also learned that Osborne had obtained an insurance policy at a previous job, and that policy designated a man named Joseph Corbett as his beneficiary.

Corbett, in turn, had a son—Joseph Corbett, Jr.—who had previously been convicted of murder but had escaped from a California prison. Now a chief suspect in the Coors case, the FBI obtained a fugitive warrant for him and placed him on the Ten Most Wanted Fugitives list soon after.

Throughout the summer of 1960, Corbett, Jr.'s trail remained cold.

But tragically, the trail leading to Adolph Coors ended on September 11, 1960, when some hikers came across a pair of trousers in the woods about 12 miles southwest of Sedalia, a town south of Denver. The pants had a key ring bearing the initials ACIII.

The trousers, other items of clothing, and skeletal remains found there were determined to belong to Coors. A jacket and shirt had bullet holes that showed he had been shot in the back, and an analysis of a shoulder bone confirmed this.

The story of Coors' disappearance remained in the public eye and was

featured in various publications, including *Reader's Digest*. Corbett, Jr.'s wanted photo sparked interest and leads across America, but it was the magazine's readers in Canada who would break the case. One reader pointed the Royal Canadian Mounted Police and their FBI allies to an apartment rented by a man who resembled Corbett, Jr., but the man had

That new information went out across Canada, and on October 29, 1960, a Vancouver police officer reported a similar vehicle parked outside of local motor inn. Soon, police—with the assistance of the FBI's Toronto legal attaché office—were knocking on the door of the hotel room. The man who answered said, "I give up. I'm the man you want."

Corbett, Jr. was returned to Colorado, where he was tried by the state for Coors' murder (because Coors' remains were found within the state, he wasn't tried on federal kidnapping charges).

During the trial, the FBI offered 23 agents, five lab examiners, and a fingerprint expert to help put forward an iron-clad case.

Especially compelling was the ransom note believed to have been typed on Corbett, Jr.'s typewriter, and damning evidence taken from his burned-out canary yellow Mercury, which was recovered by law enforcement in New Jersey shortly after Coors' disappearance. On March 19, 1961, Joseph Corbett, Jr. was convicted and sentenced to life in prison.

And 65 years later, the FBI continues to offer a wide array of investigative assistance to our state and local partners—just as we continue to rely on the support of the public to help us solve crimes.

WANTED BY THE FBI

INTERSTATE FLIGHT - MURDER
JOSEPH CORBETT, JR.

FBI No. 605,861 A

Photograph taken 1959

Photographs taken 1951

Aliases: James Barron, Joe Corbett, Walter Osborn, William Osborn, Charles Osborn, W. William Osborn, Walter Osborn and others

DESCRIPTION
Age: 31, born October 25, 1928, Seattle, Washington (not supported by birth records)
Height: 6'1" to 6'2"
Weight: 160 to 170 pounds
Build: medium
Hair: light brown
Eyes: hazel
Complexion: fair
Race: white
Nationality: American
Occupations: alkyl cooker (paint manufacturing), clerk-typist, laboratory technician, laborer, warehouseman.
Scars and Marks: mole under chin, crescent-shaped scar right thumb, scar right side of abdomen.
Remarks: allegedly left-handed and nearsighted; reported to be proficient typist and neat dresser.

Fingerprint Classification: 19 O 29 W 100 20
I 27 W 100

CRIMINAL RECORD
Corbett has been convicted of second degree murder.

CAUTION
CORBETT SHOULD BE CONSIDERED ARMED AND EXTREMELY DANGEROUS. HE REPORTEDLY IS A GUN ENTHUSIAST AND EXPERIENCED IN USE OF FIREARMS.

A Federal warrant was issued at Los Angeles, California, on March 21, 1960, charging Corbett with unlawful interstate flight to avoid confinement after conviction for murder (Title 18, U. S. Code, Section 1073).

IF YOU HAVE INFORMATION CONCERNING THIS PERSON, PLEASE NOTIFY ME OR CONTACT YOUR LOCAL FBI OFFICE. TELEPHONE NUMBER IS LISTED BELOW.

Wanted Flyer No. 241
March 22, 1960

DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
WASHINGTON 25, D. C.
TELEPHONE, NATIONAL 8-7117

Joseph Corbett, Jr.'s FBI Wanted Poster

recently moved on. The next day, the manager of a rooming house in Winnipeg called local police to report that a man who looked like the fugitive had recently stayed at her flophouse. She also noted that the suspect had been driving a fire engine red Pontiac.

Financial Fraud

Pharmaceutical Executive Sold Fake Stock in Medical Research Company



Left: Pharmaceutical executive Greg Ruehle issued fake stock certificates like this one to victims who thought they were investing in a legitimate medical research company.

money and issuing fake stock in the company.

In 2015, some of the investors asked for proof that their money was being used at the company. In response, Ruehle sent them a letter on what appeared to be ICBI letterhead, allegedly signed by the company's CEO. In truth, the letter was a forgery—Ruehle even misspelled the CEO's name.

"ICBI was completely innocent in the fraud," Roberts said, "but they were made to look bad. Certainly there was damage done to the company, which was trying to do a good thing."

Worried investors eventually contacted the FBI, and within four months, Cook and Roberts had unraveled the scheme. Last month, Ruehle pled guilty to securities fraud. In addition, he admitted to possession of a stolen firearm—discovered during the execution of a search warrant—and acknowledged that he owned three stolen firearms, all unregistered.

"There was no reason for him to be buying guns off the street when he could have been buying them legitimately from a dealer," Cook said, adding that the 64-year-old Ruehle is typical of many financial fraudsters. "He was charismatic and a natural salesman, but he used those skills to trick people. And then he used their money for gambling, to buy expensive cars, and to live on a waterfront property."

Ruehle is scheduled to be sentenced in federal court later this spring.

Greg Ruehle liked to gamble—the only problem was that he did it with other people's money. In the process, the pharmaceutical executive not only swindled his friends and people from his hometown out of millions of dollars, he injured the reputation of a legitimate medical research company.

Ruehle, a California resident who worked in the biotech industry, was hired by the medical research firm ICB International (ICBI) to identify investors who could fund its research. The San Diego-based company is developing technologies for early diagnosis and treatment of diseases such as Parkinson's and Alzheimer's.

"Basically, the company's founder invested his blood, sweat, and tears trying to come up with a cure for Parkinson's disease," said Special Agent John Roberts, who investigated the case from the FBI's San Diego Division. "He was relying on Ruehle to help raise money to move the company forward."

Instead, explained co-investigator Special Agent Bridgid Cook, Ruehle "collected nearly \$2 million

and used the money for gambling and other personal expenses."

Ruehle was not a licensed broker. He was supposed to be a finder—someone who would introduce investors to the company, and then ICBI would take it from there. But Ruehle took advantage of his hometown friends, who relied on him to provide information about the company's financial future. He took investors' money and issued them fake stock certificates, none of which he reported to ICBI.

"There were a lot of victims in this case—more than 160," Cook said, "and a major betrayal of trust." Ruehle's investors were mostly friends from Minnesota, where he grew up, and they were not wealthy. Many contributed \$5,000 or \$10,000. "He preyed upon people from his hometown," Cook explained. "They relied on his expertise and knowledge of the industry."

"Investors thought they were getting in on a great deal," Roberts added. But not one of Ruehle's investors saw a penny—and neither did ICBI. To make matters worse, the company had no idea its investment "finder" was collecting

New Top Ten Fugitive

Help Us Find a Murderer

Brenda Delgado, wanted for her role in a murder-for-hire plot that led to the death of a prominent pediatric dentist in Texas, has been named to the FBI's Ten Most Wanted Fugitives list.

A reward of up to \$100,000 is being offered for information leading directly to the arrest of Delgado, who has been described as a master manipulator and may be on the run in Mexico.

On September 2, 2015, Dr. Kendra Hatcher was murdered in the parking garage of her Dallas apartment complex. Delgado, who was studying to be a dental hygienist, is suspected of hiring two co-conspirators to carry out the murder. "Apparently she was jealous because the victim was dating her ex-boyfriend," said Special Agent Jason Ibrahim, a member of the FBI's Dallas Violent Crimes Task Force.

"Brenda Delgado was able to effectively manipulate everyone she involved in her calculated scheme," said Thomas M. Class, Sr., special agent in charge of the FBI's Dallas Division. "Although she didn't pull the trigger herself, she is still responsible for the murder," Class added, "and through international publicity and a significant reward offering, we intend to find her and to bring her to justice."

A Mexican citizen, Delgado is believed to have fled the country shortly after being interviewed by investigators about the killing. She has been charged with capital murder, and a federal fugitive warrant has been in place since October 2015. Both co-conspirators have been arrested and are in custody.

Born Brenda Berenice Delgado Reynaga, the 33-year-old fugitive

FBI TEN MOST WANTED FUGITIVE

Unlawful Flight to Avoid Prosecution - Capital Murder

BRENDA DELGADO



is described as a Hispanic female, 5 feet 5 inches tall, weighing approximately 145 pounds, with brown eyes and black hair that may be dyed a lighter color. She has a butterfly tattoo on the small of her back. Delgado has ties to Mexico, and investigators strongly believe she may be residing there. She should be considered armed and dangerous.

The search for Delgado is being coordinated by the Dallas Violent Crimes Task Force, which consists of FBI personnel and detectives from the Dallas and Garland Police Departments. Lee Thompson, a Dallas Police Department detective and member of the task force, explained that the unusual circumstances behind Hatcher's murder have drawn publicity to the case from around the world.

Delgado told one of her co-conspirators that she was connected with a cartel and could provide him with a steady source of drugs if he carried out the murder. "He thought he had an in with the cartel," Thompson said.

In the days leading up to the murder, it is believed Delgado

learned that her ex-boyfriend and Hatcher were planning a vacation to Cancun and that he had introduced Hatcher to his parents.

Delgado is the ninth woman to be placed on the FBI's Ten Most Wanted Fugitives list. Since its creation in 1950, 474 of the 506 fugitives named to the list have been apprehended or located—156 of them as a result of citizen cooperation.

We need your help: Investigators urge anyone with information concerning Delgado to take no action themselves. Instead, they should contact the FBI by calling 1-800-CALL-FBI or submitting a tip online. The FBI's Dallas Field Office can be reached at 972-559-5000. For possible sightings outside the United States, contact the nearest U.S. Embassy or Consulate.

Note: Brenda Delgado was taken into custody on April 8, 2016.

Wind Farm Investment Scam

Texas Man Sentenced to 15 Years in Federal Prison

In the midst of growing local, national, and international concerns for the environment, wind energy is one of several types of renewable energy technologies being touted as environmentally friendly. Wind energy is known as a clean, sustainable fuel source that is cost effective and widely available domestically.

So when a Texas businessman solicited investors for his renewable energy company, Wind Plus, Inc.—whose stated business goal was to find and develop land suitable for wind farm construction—he had no problem raising \$3.7 million from nearly 100 individuals in 11 states. Unfortunately for the investors, that businessman—David Lyman Spalding—was not exactly environmentally conscious, and he had no intention of following through on his business plan. Instead, he took their money

and stuffed the majority of it into his own pockets.

From at least 2003 through April 2011, Spalding worked to convince people to invest with him—sponsoring happy hours, hosting parties at his home, offering bonuses (never paid) to investors already on board who could bring in new investors. He handed out professional-looking brochures and even created a slideshow presentation for prospective investors. He explained that his company obtained land leases and the proper permits for wind farms, conducted meteorological studies to collect wind data, performed environmental studies, and obtained agreements with power companies who would have the wind farms built.

In return for their investments, Spalding offered his clients

promissory notes that said he would repay the principal back within two to 12 months, offer 10 percent interest if repayment didn't happen within that time frame, and offer shares of stock in his company if and when it went public. Unfortunately, those promissory notes weren't worth the paper they were printed on.

Spalding used most of his investors' money to fund his extravagant lifestyle—he purchased a new home, luxury vehicle, expensive jewelry, trips for him and his wife to the Caribbean and Europe, spa treatments, dinners at expensive restaurants, designer clothes, etc.

These types of schemes usually run their course when the money runs out. However, even after Wind Plus filed for bankruptcy in 2009, Spalding was able to solicit new investors for a similar renewable

energy company called Baseload Energy, LLC, which purportedly focused on geothermal energy and supposedly developed land for natural gas turbines. Like Wind Plus, Baseload Energy was just a means to an end, and that end involved Spalding scamming as many victims as possible.

Of the \$3.7 million he received during the life of his scheme, Spalding only paid out a small fraction of that back to investors—and only did that to try to keep clients from demanding their entire investments back or from filing complaints.

But eventually, one of his investors had enough and made a complaint to the FBI's Dallas Field Office in late 2010. Because of the number of victims, the financial losses, and the interstate nature of Spalding's activities, the Bureau opened a case.

Investigators conducted numerous interviews of victims and of Spalding's former employees (who had quit because they weren't getting paid). But according to the investigating agent, "financial analysis is what really made this case." She explained that since Wind Plus had no corporate records to review, FBI financial analysts went through Wind Plus bank records. These records showed that Spalding—who had no personal bank account—used company funds almost exclusively for his own benefit.

Spalding was indicted in federal court, and in April 2015—following a seven-day trial—was convicted by a jury. Last month, he was sentenced to 15 years in prison and ordered to pay more than \$3.3 million in restitution to his victims.

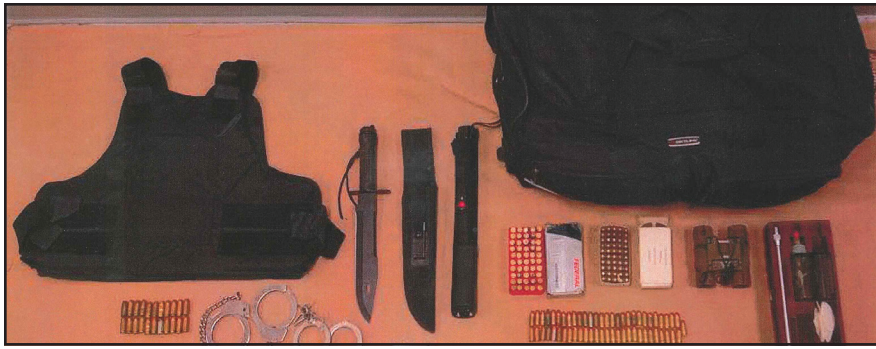
Invest Your Money Wisely: Tips for Consumers

- Be extremely cautious about unsolicited offers to invest.
- Don't believe everything you're told. Take the time to do your own research on the investment's potential—and on the person making the offer.
- Be wary of an investment opportunity that offers unusually high yields.
- Check with federal and state securities regulators to find out if there have been any complaints against the company or person you're thinking of doing business with.
- Request written financial information—such as a prospectus, annual reports, or financial statements—then compare the written information to what you were told.
- Check with a trusted financial adviser, broker, or attorney about any investments you are considering.



A Web of Intimidation

Landmark Cyberstalking Case Results in Life Sentences for Three Family Members



After surviving a rocky divorce and custody dispute in 2007, all Christine Belford wanted was to settle back into a peaceful life with her three young daughters in her Delaware home.

Instead, her ex-husband, David T. Matusiewicz, and several members of his family stalked, harassed, and intimidated Belford for years leading up to her murder at a federal courthouse in Wilmington on February 11, 2013. The ensuing investigation, conducted by the FBI and the Delaware State Police, resulted in the first-ever convictions on charges of cyberstalking resulting in death, a violation contained in the federal Violence Against Women Act.

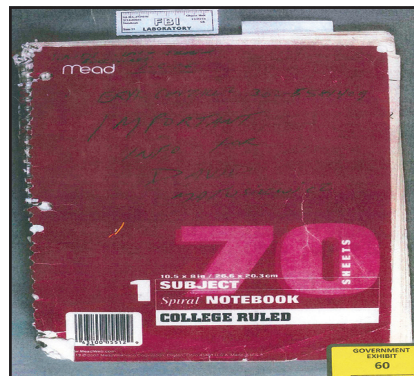
During their investigation, agents and detectives learned that David Matusiewicz hatched the plot to stalk and harass his ex-wife while in prison for kidnapping Belford's children in 2007, when the couple was going through divorce proceedings. The Delaware optometrist enlisted the help of his mother, father, and sister, who waged an elaborate, years-long, online campaign against Christine Belford, alleging she endangered the lives of the daughters she had with Matusiewicz.

"Through our investigation, we discovered that the Matusiewicz family had a network of supporters helping them uncover information

about Christine's life," said Special Agent Joseph Gordon, who investigated the case out of the Baltimore Field Office's Wilmington Resident Agency. "They were convinced by the family's claims that she was a child abuser, but they didn't know the family's real intent."

The Matusiewicz family posted false allegations on websites and YouTube and enlisted friends in their campaign. They even hired a private investigator to spy on Belford at her home. In exchanges with her family, friends, and lawyer, Belford said she feared for her life.

In August 2011, the Family Court of the State of Delaware terminated Matusiewicz's parental rights and called his allegations of abuse "baseless." In 2012, Matusiewicz petitioned the court to reduce his monthly child support payments. And in 2013, he received



A spiral-bound notebook found near the scene of the shooting contained details of the surveillance the Matusiewicz family conducted on Belford and her three children.

Left: A bulletproof vest, binoculars, restraints, weapons, and ammunition were found in vehicles near the Delaware courthouse where Thomas Matusiewicz shot and killed Christine Belford and her friend Laura Mulford.

permission to travel from Texas to Delaware for a hearing on the matter.

In February 2013, David Matusiewicz, along with his mother, Lenore Matusiewicz, and father, Thomas Matusiewicz, drove to Delaware in vehicles later found to contain weapons, ammunition, a bulletproof vest, restraints, an electric shock device, gas cans, and a shovel.

On February 11, 2013, David Matusiewicz and his father entered the courthouse lobby shortly after 8 a.m. After his son passed through security, Thomas Matusiewicz shot and killed Belford and a friend, Laura Mulford, in the lobby. David's father then ended his own life after a shootout with police.

The three surviving family members—David, Lenore, and sister Amy Gonzalez—were convicted last July on charges of conspiracy and interstate stalking resulting in death. In February, they were each sentenced to life in prison for their crimes.

"Even from their homes in Texas, the Matusiewiczes had the ability to frighten Christine through electronic and physical means," said Special Agent Gordon. "They were all responsible for her murder."

Kevin Perkins, special agent in charge of the Baltimore Field Office, called the conspiracy and stalking prosecution groundbreaking. "People who actively take part in planning crimes, even though they don't pull the trigger, will be held accountable," he said.

FBI Recognizes Leaders from Around the Nation

Director's Community Leadership Awards Presented

Today at FBI Headquarters in Washington, D.C., 56 individuals and organizations—all leaders within their communities—were recognized by Director James Comey on their extraordinary contributions to education and to the prevention of crime and violence within their communities.

Comey called today “one of the very best days in the FBI’s year.”

Each recipient received the Director’s Community Leadership Award, presented every year since 1990 by FBI field offices around the country to publicly honor those who have gone above and beyond the call to service by tirelessly working to make their own cities and towns a better and safer place for their fellow residents.

The 2015 award recipients come from all backgrounds, all professions, and all parts of the country, and the issues they focus on vary greatly. But according to Comey, “They are united by a single thing—an effort to do good.”

Comey explained why the FBI publicly recognizes community leaders in this annual ceremony. “First,” he said, “we want to thank them, because they’re doing the same things we’re doing, which is trying to make life better for the American people.”

“And secondly,” added Comey, “we want to show the world what America looks like...and that this is what we do in communities all over the country.” He also hopes that the honorees inspire others, especially young people, to follow in their footsteps.

Among the individuals and organizations recognized during 2015 by FBI field offices were:



Recipients of the 2015 Director's Community Leadership Awards were celebrated at FBI Headquarters in Washington, D.C.

Anchorage: Samuel Johns, for helping homeless Alaskan native reconnect with their families, friends, and culture through Forget Me Not, the non-profit organization he founded.

Baltimore: Operation Pulse (People United to Live in a Safe Environment), for its work to reduce violent crime in and around East Baltimore through a variety of crime prevention programs for churches, senior groups, churches, and businesses.

Honolulu: Roy Sakuma, who for the past 50 years has taught, mentored, inspired, and brought hope to thousands of people in Hawaii and even Japan, and who has spent countless hours speaking to school children, candidly sharing his experiences regarding bullying, suicide, and insecurity.

Los Angeles: Omar Siddiqui, for bringing Muslim community leaders to the table to meet with Los Angeles FBI representatives and for encouraging young Muslim adults to participate in FBI-sponsored community outreach programs.

Memphis: Zulfat Suara, for her work with students in Hardeman

County involving the Junior Achievement Program, which teaches students skills like managing finances and making good career choices.

San Francisco: The KlaasKids Foundation, established by the family of murder victim Polly Klaas, for its efforts in locating and assisting children exploited by perpetrators of child sex crimes in the Bay area.

St. Louis: The Fortune 500 company Emerson, through its Ferguson Forward initiative, for donating \$8.5 million and operating 30 programs—focused on areas like early childhood education, youth jobs, college scholarships, and technical and trade careers—for the young people of Ferguson and North St. Louis County, Missouri.

A special thanks to the winners for giving of their time and talents to enhance the lives of others.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/dcla2015.

Man Gets 16 Years for Attempting to Purchase Ricin

Use of Stolen Identity Adds to Length of Sentence



Left: The shipment sent by the FBI to Cheng Le contained, among other things, a pill bottle holding a single phony ricin tablet.

It was a very scary scenario: Chinese national Cheng Le, living in New York City, attempted to order ricin through the so-called dark web.

Ricin, of course, is a highly potent and potentially fatal toxin with no known antidote. And the dark web includes a number of extensive, sophisticated, and widely used online criminal marketplaces that allow participants to buy and sell all kinds of illegal and often dangerous items, including drugs, firearms, and hazardous materials, like ricin.

What did Le plan to do with the ricin? Nothing good. According to U.S. Attorney for the Southern District of New York Preet Bharara, “In Le’s own words, established at trial, he was looking for ‘simple and easy death pills’ and ways to commit ‘100 percent risk-free’ murder.”

While on a particular dark web marketplace in early December 2014, Le asked, “This might sound blunt but do you sell ricin?” Fortunately, the individual at the computer on the other end was not a trafficker in lethal poisons—instead, it was an undercover FBI employee.

For the next couple of weeks or so, Le and the undercover employee exchanged more than 20 encrypted messages. Some of Le’s

communications included:

- “If [the ricin’s] good quality, I’ve already had buyers lining up.”
- “Does ricin have an antidote? Last I check there isn’t one, isn’t it?”
- “The client would like to know... if it is wise to use ricin on someone who is hospitalized... Injection will leave needle holes on the body which could be found in regular forensic examinations. But hospitalized people already have needles in them so it wouldn’t be suspicious...”
- “I’ll be trying out new methods in the future. After all, it is death itself we’re selling here, and the more risk-free, the more efficient we can make it, the better.”
- “Also, besides that one bottle of pills with one poisonous pill in there, can you send some extra loose powder/liquid ricin? I’d like to test something.”

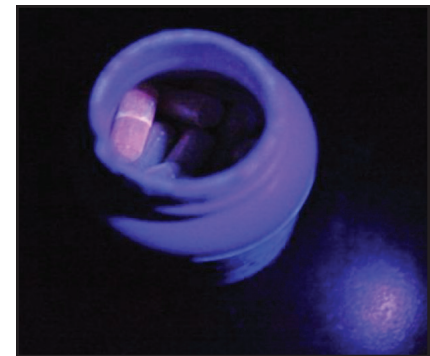
Sometime during these exchanges, Le revealed to the undercover employee that he had a specific victim in mind: “Someone middle-aged. Weight around 200 pounds.”

Ultimately, Le placed his order, paying with bitcoins, a virtual currency. Bitcoins themselves are not illegal and have known legitimate uses. However, they are also a common form of payment for illegal goods and services on the dark web because of the anonymity they provide.

On December 18, 2014, Le directed his contact to send a quantity of ricin to a rented postal box at a Manhattan shipping store

(investigators later determined that Le had rented the postal box using the name of an individual whose identity he had stolen).

The Bureau prepared a mock shipment exactly as Le had requested—with one small difference: the “ricin pill” concealed in a pill bottle and the loose “ricin powder” were fake. And on December 23, the sham shipment was delivered to the requested postal box. Le, wearing latex gloves, retrieved the package, opened it, and took it to his apartment. Agents, armed with a search warrant, entered the apartment, collected the evidence, and arrested Le.



The phony pill sent to Le glows under ultraviolet light, just as real ricin would.

Le was tried by a federal jury and convicted in August 2015 of, among other things, attempting to possess a biological toxin for use as a weapon and aggravated identity theft in relation to a terrorism offense. Last month, he was sentenced to 16 years in prison, a term that had been enhanced by the aggravated identity theft charge.

And as a result of yet another successful joint law enforcement investigation—this one by the FBI, New York Police Department, and U.S. Postal Inspection Service—a criminal who posed a deadly threat to the public is behind bars.

Violent Home Invasion

Case Illustrates Threat Posed by Gangs

Violent gangs pose a significant threat to communities throughout the United States. You don't have to live in South Central Los Angeles or Chicago's inner city to feel the impact of gang violence, as a recent case from Washington state illustrates.

On a Tuesday evening in November 2014, three teenagers from Seattle's Down with the Crew Gang—a violent affiliate of the Black Gangster Disciples gang—set out from Seattle for a 50-mile drive south to the community of Lakewood. Their intention was to rob a large-scale drug house they had received information about.

Around 9:30 p.m., a 66-year-old Lakewood man answered a knock at his door and was confronted by the three youths, who forced their way into the home. The gang members had picked the wrong house, but that didn't matter to them. What happened next was 20 minutes of terror for an innocent couple.

The gang members pistol-whipped the man until he was unconscious, tied his hands, and placed a blanket over him. They broke down a bathroom door and dragged out his 61-year-old wife, stabbed her, tied her hands, and placed her under the blanket with her husband, who was bleeding severely.

"They brutalized the couple," said Special Agent Kelly Smith, who supervises the South Sound Gang Task Force—one of more than 160 FBI-led Safe Streets task forces nationwide—which handled the investigation out of the Bureau's Seattle Division. "The level of violence and complete disregard for human life was astounding in this case," he added.



Gang members shot through the front door of a Washington couple's house during a violent home invasion in November 2014.

That disregard for life became even more apparent as the home invasion continued. The robbers were in and out of the house carrying stolen items to their car when the husband regained consciousness. He was able to free himself and his wife, and with all three assailants temporarily outside, he locked the front door and the couple retreated to their bedroom, where he called 911 and retrieved his handgun.

The robbers forced their way back inside, firing a gunshot through the front door. Then they kicked down the locked bedroom door where the couple had barricaded themselves behind their bed. Confronted again by the attackers, the man fired two shots, hitting 19-year-old Taijon Vorhees both times.

At that point, all three robbers fled and drove away. And the two uninjured gang members—Duprea Wilson and Qiuordai Taylor, ages 19 and 17, respectively—decided to help themselves rather than their wounded friend.

"They didn't want anything to do with taking him to a hospital," said Jeff Martin, a Lakewood Police Department detective assigned to the South Sound Gang Task Force. "They drove around until

he was unconscious, then dumped his body and left him to die. They basically pushed him right out of the car."

The wounded teen did, in fact, die. The two other subjects were apprehended within 72 hours of the crime. At trial in February 2015, the two surviving defendants faced 11 state felony charges. One of the charges was manslaughter—for allowing their friend to die without seeking medical attention.

In March 2016 a jury found Wilson and Taylor guilty on all counts, and later that month a judge sentenced them each to 56 years in prison.

Smith, who has supervised the task force since 2012, credits his local, state, and federal partners, along with experienced Pierce County Prosecutor's Office attorneys, with bringing the case to a successful conclusion.

As for the victims, Martin said they have mostly recovered from their physical injuries, but there are still emotional issues to contend with. "There are definitely lasting effects from the attack," he said, "maybe effects that will last the rest of their lives."

Sextortion and Cyberstalking

How a Single Tip Uncovered an International Scheme



The investigation that uncovered a far-reaching sextortion scheme by a U.S. State Department employee at the U.S. Embassy in London all started with a single complaint by a young victim in Kentucky. She went to the police.

“The victim basically was saying that she was being cyberstalked by some guy who got into her e-mail and was threatening to expose compromising photos of her to her friends and family,” said FBI Special Agent Andrew Young, who interviewed some of the hundreds of victims targeted by Michael C. Ford, a former State Department civilian employee who was sentenced last month to nearly five years in prison for hacking into the e-mail accounts of young women to extort them.

According to the facts of the case, between January 2013 and May 2015, Ford—while working in London—posed as a member of a large web company’s “account deletion team” and sent out e-mails to thousands of women warning them that their e-mail accounts would be deleted if they didn’t provide their passwords. Ford then used the passwords he received to hack into victims’ e-mail and social media accounts to search for nude

and topless photos and personal information like contacts and addresses.

He hacked into at least 450 e-mail accounts and admitted e-mailing at least 75 women, threatening to circulate their compromising pictures unless they sent him more.

Following the initial complaint in Kentucky, local police reached out to the FBI in Louisville, where agents traced the source of the e-mails to a State Department server in London. The Diplomatic Security Service (DSS) began an internal probe that led to Ford and uncovered the massive hacking, cyberstalking, and sextortion scheme. Young said the investigation showed Ford spent the bulk of his time at work using a government computer to “extort women, hack into their e-mail accounts, and threaten them.”

The FBI’s primary role in the investigation was interviewing victims across the U.S. to build a case. “They were angry,” said Young, who worked the case out of the FBI’s Atlanta Field Office, which had jurisdiction because Ford had Georgia residency. “Somebody steals your most private pictures out of your computer, then

comes back and threatens you with it. They felt compromised.”

At Ford’s March 21 sentencing, prosecutors presented evidence of another scheme he started several years earlier, in 2009. Posing as a talent scout, Ford combed through websites where aspiring models posted their pictures and contact information. He duped young women into sending personal information, including their measurements and dates of birth. “He would send them an e-mail with a link, and when they clicked on the link he got access to their computer and e-mail accounts,” Young said.

Ford, 36, of Atlanta, was indicted August 18, 2015 following his arrest by DSS during a visit to Atlanta. He pled guilty in December.

His plea was due in large part to the voluminous evidence against him, including the statements of victims like the one who came forward in Kentucky.

“There was no getting around it,” Young said. “Witness after witness and a lot of forensic evidence—it made putting him in jail a whole lot easier.”

Incidents of Ransomware on the Rise

Protect Yourself and Your Organization



Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted recently by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.

The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and

files, and the potential harm to an organization's reputation.

And, of course, home computers are just as susceptible to ransomware, and the loss of access to personal and often irreplaceable items—including family photos, videos, and other data—can be devastating for individuals as well.

Ransomware has been around for a few years, but during 2015, law enforcement saw an increase in these types of cyber attacks, particularly against organizations because the payoffs are higher. And if the first three months of this year are any indication, the number of ransomware incidents—and

the ensuing damage they cause—will grow even more in 2016 if individuals and organizations don't prepare for these attacks in advance.

In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.

Once the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam e-mails, but because e-mail systems got better at filtering out spam, cyber criminals turned to spear phishing e-mails targeting specific individuals.

And in newly identified instances of ransomware, some cyber criminals aren't using e-mails at all. According to FBI Cyber Division Assistant Director James Trainor, "These criminals have evolved over time and now bypass the need for an individual to click on a link. They do this by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers."

The FBI doesn't support paying a ransom in response to a ransomware attack. Said Trainor, "Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current

cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."

So what does the FBI recommend? As ransomware techniques and malware continue to evolve—and because it's difficult to detect a ransomware compromise before it's too late—organizations in particular should focus on two main areas:

- Prevention efforts—both in terms of awareness training for employees and robust technical prevention controls; and
- The creation of a solid business continuity plan in the event of a ransomware attack. (See sidebar.)

"There's no one method or tool that will completely protect you or your organization from a ransomware attack," said Trainor. "But contingency and remediation planning is crucial to business recovery and continuity—and these plans should be tested regularly." In the meantime, according to Trainor, the FBI will continue working with its local, federal, international, and private sector partners to combat ransomware and other cyber threats.

If you think you or your organization have been the victim of ransomware, contact your local FBI field office and report the incident to the Bureau's Internet Crime Complaint Center.

Tips for Dealing with the Ransomware Threat

While the below tips are primarily aimed at organizations and their employees, some are also applicable to individual users.

Prevention Efforts

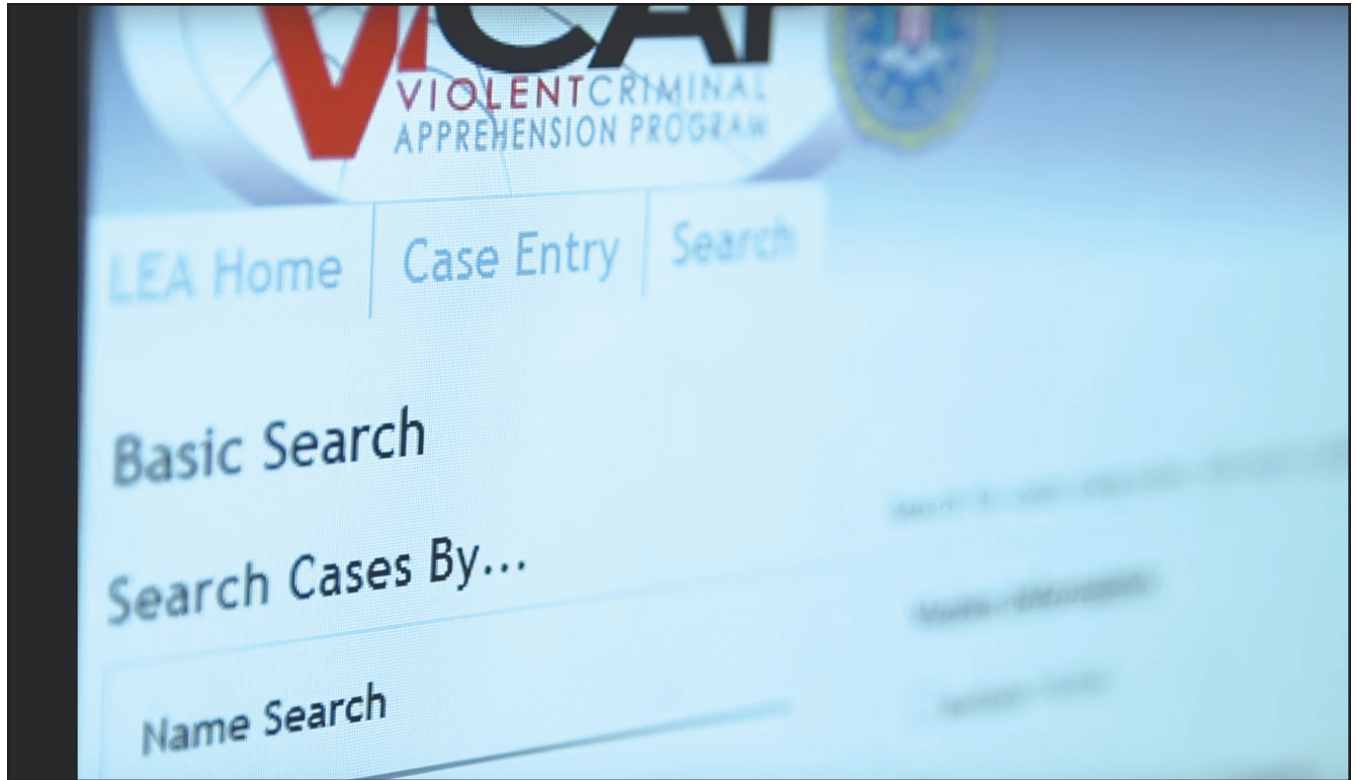
- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.
- Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).

Business Continuity Efforts

- Back up data regularly and verify the integrity of those backups regularly.
- Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

Violent Criminal Apprehension Program

Part 1: Sharing Information to Stop Serial Offenders



The homicide investigators, crime analysts, intelligence analysts, and administrators in the police department classroom studied their computer monitors, ready to receive instruction on—and access to—a powerful database that serves as a nationwide repository for certain types of violent crimes.

The men and women from regional law enforcement agencies were gathered in Scottsdale, Arizona for an introduction to the FBI's Violent Criminal Apprehension Program (ViCAP), whose mission is simple: share information to help solve serial crimes.

“ViCAP Web is the only national law enforcement database that contains both investigative and behavioral information related to specific types of cases,” said Rick Blankenship, an FBI crime analyst who travels the country to train law enforcement on the use of the system. “We are not looking for

law enforcement agencies to enter every one of their homicides or sexual assaults in ViCAP Web,” he explained. “We are looking for cases of a serial nature, where we think this may not have been the first time the offender committed this type of crime.”

The detailed information entered about each of the approximately 85,000 cases in the system allows investigators to find potential links to their own case—all while sitting at their office computers. “If you are a small police department investigating a murder case, how do you know if it’s a serial crime?” Blankenship asked. “ViCAP is where you can go for help.”

Investigators from across the country—many from small agencies that don’t usually see violent serial crimes—can enter their cases in ViCAP Web and search the system for similarities with other cases. Did the offender



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/vicap1.

pose the victim in a particular way? Did he choose a particular kind of victim, like a prostitute or an elderly person? Were certain items removed from the crime scene? Was DNA recovered? If the database shows that a peculiar sexual homicide in Chicago was similar to a previous case in upstate New York, for example, it might provide investigators from both jurisdictions with new leads and possible suspects.

“A lot of times local law enforcement gets involved in a case and they hit a wall where they don’t have any more leads,” said Thomas E. Kelly, chief of the Apache Junction Police Department near Phoenix, who has been using and promoting the database for several years.

“ViCAP Web allows investigators to compare incident details with thousands of other cases. And every time a new case comes into the system, it’s compared to the case that you submitted, so cases are constantly being reviewed for any connections.”

Nearly 5,500 U.S. law enforcement agencies participate in the program. Cases that meet the ViCAP criteria—including homicides and attempted homicides, sexual assaults, missing persons, and unidentified human remains—are entered and include details about the crime, the victim, and whatever is known about the offender. The database can be searched using various keywords and filters. If an investigator is working a murder case where the victim was shot, stabbed, and bound, he can search ViCAP Web for cases where victims were killed in the same way.

ViCAP analysts like Blankenship and Christie Palazzolo, who also provided instruction at the recent Arizona training, specialize in violent serial crimes and monitor the database with their colleagues from their FBI offices in Virginia. They regularly provide consultative and analytical services to investigators.

“Many smaller agencies might not have crime analysts,” Blankenship said. “When they come across one of these types of cases, they can place it in ViCAP and it gives them the opportunity to use our resources. We can do the analytical work for them and provide investigative leads and contacts with other agencies who have similar cases.”

Blankenship added that ViCAP Web is a free service provided

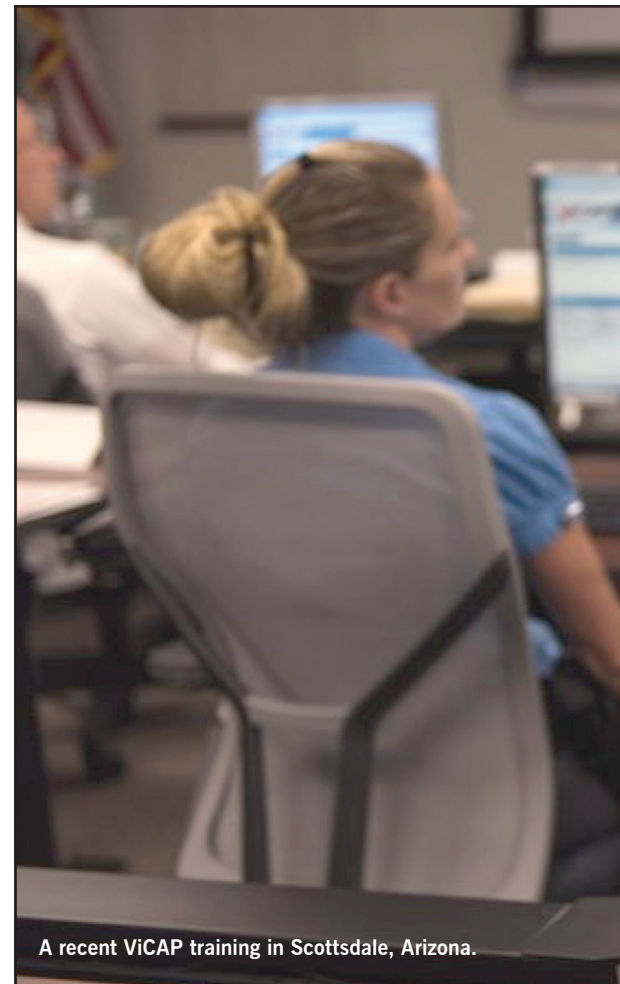
by the FBI and is open to law enforcement agencies nationwide. The only “cost” for training and access to the system is that participating agencies must enter their criteria cases so that the database continues to expand.

At the training session in Scottsdale, law enforcement personnel learned about the system by entering their cases. An officer from Flagstaff brought a cold case homicide from his department. A deputy from a different jurisdiction entered her sexual assault case. A detective from the Scottsdale Police Department who was familiar with ViCAP because of a murder case he has been working for the past year (see sidebar) encouraged his colleagues to receive the training and get access to the database.

“We are constantly looking for more agencies to join ViCAP,” Blankenship said. “When we go out and train law enforcement personnel and they see what ViCAP can do and how easy it is to get the information into the system, they get excited about being able to move their cases forward.”

In addition to the database, which is a part of the FBI’s National Center for the Analysis of Violent Crime (see sidebar), FBI analysts offer a range of other free services to help investigators.

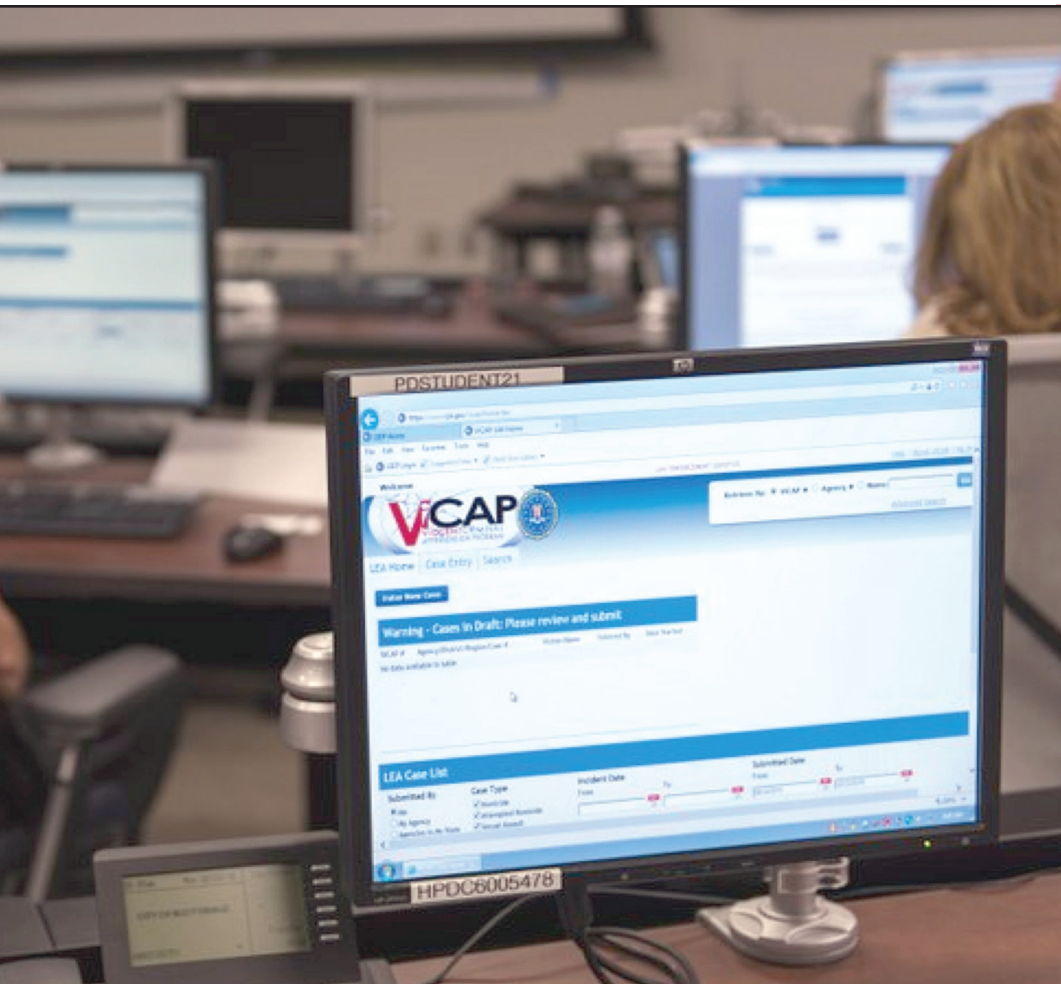
“There’s more than just the database,” said Kelly, the Apache Junction police chief. “We had an unidentified victim where we just had skeleton remains. My crime scene technician contacted the Bureau, and they did a facial reconstruction. With a likeness of the victim, we then reached out to the media and asked for the public’s help to identify her. Once you are



A recent ViCAP training in Scottsdale, Arizona.

in the program,” he noted, “there is a lot of help available.”

“The bottom line,” Blankenship said, “is that we are all in this together. The more resources you can throw at solving a crime, the better your chances are of solving it. We want law enforcement agencies to know that we’re here to help them, and we want the public to know that these cases are not forgotten. There’s always the possibility that the newest case that comes in will match up with a case from five or 10 years ago,” he explained. “We want the public to know—especially the families of victims—that we are constantly looking at these cases.”



National Center for the Analysis of Violent Crime

The Violent Criminal Apprehension Program (ViCAP) is part of the FBI's National Center for the Analysis of Violent Crime (NCAVC). The primary mission of the NCAVC is to provide behavioral-based investigative support to the FBI, national security agencies, and other federal, state, local, and international law enforcement involved in the investigation of unusual or repetitive violent crimes, threats, terrorism, cyber crimes, public corruption, and other matters.

The NCAVC consists of five Behavioral Analysis Units (BAU), each of which offers investigative and operational support to complex and time-sensitive crimes in distinct areas:

- BAU-1: National security matters, including counterterrorism, arson, and bombings
- BAU-2: Threat assessment, cyber crimes, and public corruption
- BAU-3: Crimes against children
- BAU-4: Crimes against adults/ ViCAP
- BAU-5: Research, strategy, and instruction

The Allison Feldman Murder Case

On a Tuesday evening in February 2015, someone entered the home of Allison Feldman, a 31-year-old who lived alone in Scottsdale, Arizona. The offender violently attacked her, and she died from her injuries.

"We know from evidence obtained at the scene that the suspect was in the home for some time," said T.R. Davidson, a homicide sergeant with the Scottsdale Police Department. "The violence and the countermeasures the offender used led us to believe that this may not have been his first offense."

Davidson (right) immediately entered the case into the FBI's ViCAP system, hoping to find cases with similar circumstances in other jurisdictions. "So far, we have not come up with anything linking her case to any others," he said, "but there may be that other case we come across that will allow us to link them and develop new information. That could help us solve this crime."

None of the typical leads in the case have panned out, Davidson noted. "In going through all her friends and contact lists and associates and work people, we've identified nothing out of the ordinary, nothing that would lead us to believe that this was someone that she knew. We believe that Allison did not know her attacker. And that leads us to believe that the offender may have done this before or may re-offend."

Using the ViCAP system is one more resource for Davidson. "The more information we have, the more we learn about other cases, the more likely we are to develop new information about a potential offender," he explained. "This case has been the number one priority for the Scottsdale Police Department for the past year. We are leaving no stone unturned."

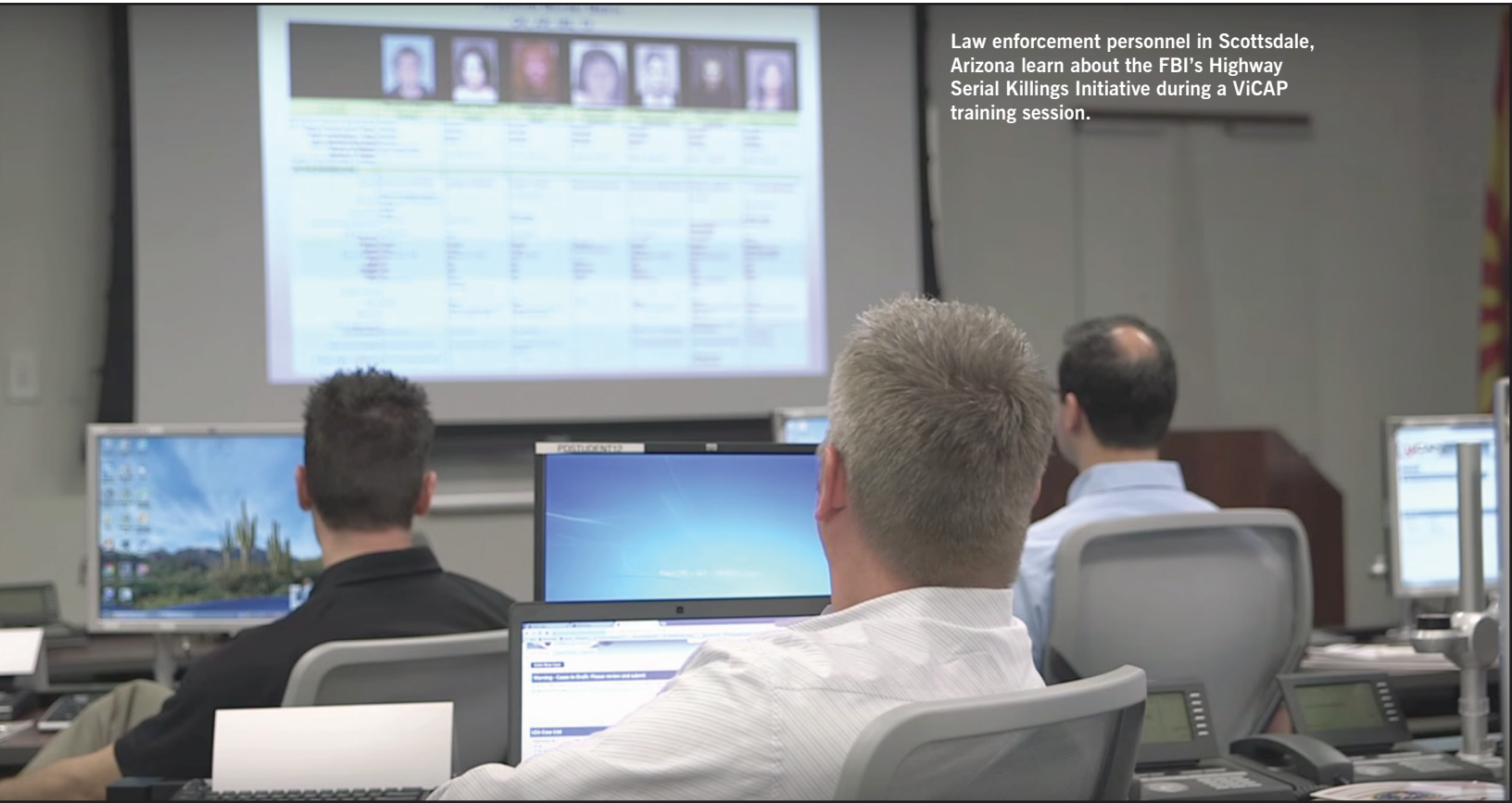
Davidson and his colleagues took part in the recent ViCAP training so they can better understand how the database works. "ViCAP is not necessarily something that you turn on and get something right away," he said. "It's something that may be fruitful down the road. It may give us additional information or leads that will allow us to solve this case."

Anyone with information about the Feldman murder is urged to contact the Scottsdale Police Department at (480) 312-5000 or the Silent Witness organization, which is offering a \$10,000 reward for information that leads to the arrest of the killer. Call the Silent Witness hotline at (480) 948-6377, or visit silentwitness.org.



Violent Criminal Apprehension Program

Part 2: The Highway Serial Killings Initiative



Law enforcement personnel in Scottsdale, Arizona learn about the FBI's Highway Serial Killings Initiative during a ViCAP training session.

If there is such a thing as an ideal profession for a serial killer, it may well be as a long-haul truck driver.

FBI Crime Analyst Christie Palazzolo is quick to point out that long-haul trucking is an honorable profession and that the overwhelming majority of drivers are not murderers—but it does happen, and the pattern is unmistakable.

More than a decade ago, analysts for the FBI's Violent Criminal Apprehension Program (ViCAP)—the only national database of serial crimes—began to see a marked increase in the number of bodies recovered along the side of the road. A majority of the victims were truck-stop prostitutes, and it turned out that many of the suspects were long-haul truckers. “We had an inordinate number of victims and offenders from this

rather specific population pool,” Palazzolo explained.

To make matters worse, these cases are extremely difficult to investigate. A long-haul driver can pick up a prostitute at a truck stop in Georgia, rape and murder her, and dump her body on the side of the road in Florida later that day. The victim has no connection to the area where she was found, and there may be no forensic evidence to collect because the crime was committed hundreds of miles away. The local police detectives investigating the case might have little experience dealing with a crime of this nature and may be faced with few, if any, leads.

To raise awareness among law enforcement agencies—and the public—about highway serial killings, and to focus ViCAP resources on helping to solve these cases, in 2004 the FBI began the

Highway Serial Killings (HSK) Initiative, with support from the trucking industry.

“We want to help local law enforcement agencies tie their cases to similar cases nationwide,” said Palazzolo, who has been managing the initiative for the past four years. “That’s where ViCAP comes in, because the database can make those connections.”

Without ViCAP—part of the FBI's National Center for the Analysis of Violent Crime—local law enforcement agencies investigating one of these cases may have no way of knowing a murder in their jurisdiction is similar to killings committed elsewhere. Since the initiative began, ViCAP analysts have compiled a list of more than 750 murder victims found along or near U.S. highways, as well as nearly 450 potential suspects.



Since the Highway Serial Killings Initiative began in 2004, ViCAP analysts have compiled a list of more than 750 murder victims found along or near U.S. highways, as well as nearly 450 potential suspects.

The analysts also began to develop detailed timelines on many of the suspects. The information in the timelines, obtained from company logs, gas station receipts, and other records, helps investigators pinpoint where a suspect was when murders were committed.

"It's not unusual for a driver to pass through five or even seven states in one day," Palazzolo said. "The amount of ground they cover and the lack of any connection to where they're passing through makes it difficult to tie cases back to them."

So the timelines become crucial to investigations. The goal for ViCAP analysts is to obtain as many records from as many sources as possible to determine a driver's whereabouts at fixed points in time.

"Those details are what ultimately will help tie the suspect back to the murders," Palazzolo said.

The database is constantly monitored for cases that meet the HSK criteria. When cases are identified, ViCAP analysts can provide information to local law enforcement agencies regarding these cases—anything from timeline data to advice on what records to subpoena to suggesting a point of contact at another police department with similar cases.

In the 12 years since its creation, the Highway Serial Killings Initiative has helped many local police departments solve violent sexual assaults and murder cases, but Palazzolo cautioned that many more victims demand justice. And

these highly mobile killers are not going to disappear.

"According to the Department of Transportation," she said, "the number of truck drivers on the road in the next 20 years is going to grow exponentially. So if we've already identified a population from which we are getting a significant number of offenders, and if we are going to be seeing more and more trucks on the road, the potential for additional highway serial killings is definitely there."



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/vicap2.

Child Sexual Exploitation

Threat from Pedophiles Online is 'Vast and Extensive'



The case of a Tennessee man sentenced last month to 21 years in prison on child pornography charges serves as an important reminder to parents and children about the dangers of an online world where things are not always as they appear and pedophiles may be lurking around many virtual corners.

Brian K. Hendrix was convicted earlier this year in connection with his operation of two websites whose sole purpose was to trick children into engaging in sexually explicit activity that he and his co-conspirators were secretly recording. An investigation identified more than 300 American children who were victims—some as young as 8 years old—and an estimated 1,600 other youths who were lured to the websites.

The pedophiles tricked their young victims by creating fake profiles on social networking sites, where they posed as teenagers to lure children to their websites. When the youngsters landed on the sites, the 42-year-old Hendrix and his criminal colleagues showed them pre-recorded sexual videos of prior victims to make the new victims think they were chatting with their peers.

Once lured to the websites, the criminals—masquerading as teens—used sophisticated psychological tactics to coerce

many of the children to engage in sexually explicit activity using the cameras on their tablets, smartphones, and desktop computers—all of which the adults recorded.

“Hendrix was one of several main members of the conspiracy,” said Special Agent Paul Cha of the FBI’s Violent Crimes Against Children Section. “Pedophiles are very active online,” he said. “Their numbers are vast, and their reach is extensive. They track children’s activities. When they realized how popular chat sites are with children, they found a way to exploit it.”

The FBI-led investigation, dubbed Operation Subterfuge, has thus far resulted in the conviction of eight others besides Hendrix, with average prison sentences ranging between 18 and 21 years. Cha explained that most of the children caught up in the exploitation had no idea they had been victimized.

The majority of the victims were American, but victims were also located in Canada and several other countries. Because of the large number of children impacted, investigators enlisted the help of the FBI’s Office for Victim Assistance to inform parents about the crimes and to offer assistance. When contacted by the FBI, Cha said, “Many of the parents were in complete shock.”

The victims and their families came from all social and economic backgrounds, according to Special Agent Daniel Johns, an Operation Subterfuge investigator. “There were victims who came from good homes with very active, stable parents.”

Pedophiles are experts at grooming and coercing youngsters, Johns said, and sometimes as many as 20 adults posing as teens were on the websites, manipulating children. “Their coercive tactics—that constant barrage on a child’s mind—succeeded in breaking down their barriers,” he said. “These tactics have been perfected by predators to make a child feel bad. And the adults were all working together. In a lot of cases, the kids really didn’t stand a chance.”

Johns, a veteran child exploitation investigator, said this case represented a level of sophistication on the part of pedophiles he has never seen before. “From creating their own website to giving that website the ability to record the criminal activity and then to be able to download it—along with the sophistication, coordination, and grooming to be able to break down all the child’s barriers—is disconcerting.”

Increasingly, children of all ages own or have access to devices that allow them to get online. Johns urges parents to follow a few simple rules when it comes to social networking sites and Internet usage in general for children: “Tell your kids that if they haven’t met the person in real life, they shouldn’t be friends online,” he said, adding, “Limit your child’s device usage to common areas of the household, and store those devices in your bedroom at night.”

Human Rights

FBI Reaching Out About Female Genital Mutilation

More than 500,000 women and girls across the country—most of them living in metropolitan areas—are at risk of undergoing female genital mutilation, a procedure that has long been practiced in many African and Middle Eastern countries as a cultural custom but has been illegal in the U.S. since 1996.

A report showing the number of women at risk was published in January by the Centers for Disease Control and Prevention, and the figure was much higher than previously estimated. A separate report last year by the non-profit Population Reference Bureau (PRB) determined that women and girls most at risk were concentrated in major cities like New York, Minneapolis, Los Angeles, and Washington, D.C., where large diaspora immigrant communities have coalesced.

Female genital mutilation, also called cutting or FGM, involves partial or total removal of the external genitalia for non-medical reasons, with no discernible health benefits. Nearly one-third of the estimated 513,000 women at risk are under the age of 18, according to the CDC and PRB data.

The FBI is proactively investigating tips and leads on this illegal practice. Investigators are hoping victims and community members who are opposed to it will come forward and report cases.

Earlier this year, the FBI and U.S. Immigration and Customs Enforcement (ICE) recognized the International Day of Zero Tolerance for Female Genital Mutilation (February 6) in a joint statement calling for eradication of the practice. The United Nations leads the zero-tolerance campaign,

estimating that at least 200 million girls and women alive today have undergone some form of FGM.

Last July, President Barack Obama elevated the issue during a speech in Kenya. “There’s no excuse for sexual assault or domestic violence, there’s no reason that young girls should suffer genital mutilation, there’s no place in a civilized society for the early or forced marriage of children,” Obama said. “These traditions may go back centuries; they have no place in the 21st century.”

Practitioners claim they are abiding by deeply rooted beliefs and traditions. But it is more broadly seen as a human-rights violation. “It reflects deep-rooted inequality between the sexes and constitutes an extreme form of discrimination against women and girls,” the U.N. said in a statement.

“We want people to know that the FBI is committed to preventing FGM within the United States.”

Despite being a criminal violation in the U.S., the practice continues in a variety of ways. “We believe some of it is being conducted by medical practitioners—physicians, nurses, midwives—and some by female elders within the communities who have the distinction of being what is called a cutter,” said Special Agent Kerry Sparks, who focuses on FGM cases as part of the FBI’s International Human Rights Unit (IHRU).

A State Department video released in February, to coincide with the International Day of Zero Tolerance for Female Genital Mutilation, highlights stories of

survivors and the role community leaders have in ending FGM.

After legislation banning FGM in the U.S. was passed in 1996, some young women were sent on trips to their home countries to have the procedure. In 2012, Congress passed additional legislation, the Transport for Female Genital Mutilation Act, making so-called “vacation cutting” illegal.

In 2005, two Southern California individuals pled guilty to charges related to a plot to allegedly perform FGM on two minors. In 2006, an Ethiopian man living in Georgia was convicted on charges of aggravated battery and cruelty to children for performing FGM on his 2-year-old daughter.

Unfortunately, it is a rare occasion when someone steps forward to report this crime to law enforcement. Most states don’t have their own laws criminalizing FGM, so many people may not know it’s a federal violation.

“A lot of our efforts focus on increasing community awareness,” said Thomas Bishop, chief of the IHRU. “We want people to know that the FBI is committed to preventing FGM within the United States.”

Anyone who has information about an individual who is suspected of assisting or facilitating the practice of FGM is urged to submit a tip at tips.fbi.gov.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/fgm.

Countering Terrorism

Inside the Mufid Elfgeeh Investigation



Left: Mufid Elfgeeh was arrested in 2014 when he took possession of two handguns and two silencers he bought for \$1,000. In March, he was sentenced to 270 months in prison for his role in supporting ISIL.

A New York man was recently sentenced to more than 22 years in prison for attempting to provide material support to the Islamic State of Iraq and the Levant (ISIL)—and an FBI investigation revealed that he was dangerously close to shifting from support to violent jihad on U.S. soil.

Described as one of the first ISIL recruiters ever apprehended, 32-year-old Mufid Elfgeeh was arrested in Rochester in May 2014, just weeks after ISIL had been officially designated a terrorist organization.

Born in Northern Yemen, where he was introduced to radical Muslim teaching at an early age, Elfgeeh moved to Brooklyn, New York as a teenager to be with his father and later relocated to Rochester, where he ran a small pizza shop.

He became increasingly outspoken about his radical religious beliefs—so much so that he was asked to leave three different Rochester mosques, according to FBI agents who investigated the case out of the Bureau's Buffalo Division. In late 2013, a concerned individual in the community—and a trusted

FBI source—alerted members of the Rochester Joint Terrorism Task Force (JTTF) about Elfgeeh's actions.

Elfgeeh actively recruited and attempted to send two individuals to Syria to fight on behalf of ISIL. He sent anti-American ISIL propaganda videos to one of the individuals and paid for his passport. He provided guidance about traveling to Syria, along with an overseas contact to coordinate the trip. Fortunately, both individuals were cooperating with the investigation. Elfgeeh also sent \$600 to a third man in Yemen to travel to Syria to fight for ISIL.

In addition, he used social media to declare his support for violent jihad and ISIL, and encouraged others to do the same. Unbeknownst to Elfgeeh, though, JTTF investigators were monitoring his every move.

During the 18-month investigation, Elfgeeh started to see himself as more than a facilitator and began discussing targeting U.S. servicemen. "Killing U.S. veterans was justified in his mind," said an FBI agent assigned to the investigation. "He had stated, 'we

kill them as they kill us.' " Later, Elfgeeh approached an individual he believed was a fellow jihadist—who was cooperating with the FBI—and wanted to buy weapons.

"He had debts and little money," said the FBI agent, "but he came up with a \$1,000 to buy two handguns and two silencers, money that should have gone to paying his next month's restaurant bills. At that point," the agent added, "the investigation changed—from a guy who was providing financial support and attempting to recruit people, to someone who was planning an attack. In our minds he was in the final stages of an operation. Nobody gets two guns with silencers for personal protection."

JTTF investigators arranged for the gun purchase—real handguns that were rendered safe so they could not be fired. When Elfgeeh took possession of the weapons, he was arrested. "We knew we had to get him off the street," the agent said.

Elfgeeh was indicted on a variety of charges stemming from his terrorist activities, and in December 2015 he pleaded guilty to his role in providing support to ISIL. In March 2016, he was sentenced to 270 months in prison.

The FBI agent who supervised the investigation credits local, state, and federal JTTF partners with their tireless efforts in bringing Elfgeeh to justice and making sure he was not able to hurt anyone. "Everyone in the community recognized that he was a threat to public safety," he said.

New Top Ten Fugitives

Help Us Find Two Murderers

Two men charged with brutal murders have been named to the FBI's Ten Most Wanted Fugitives list, with rewards of up to \$100,000 being offered in each case.

Philip Patrick Policarpio is wanted for the murder of his pregnant girlfriend in Los Angeles on April 12, 2016. At the time of the killing, Policarpio was on parole for a conviction in 2001.

Also added to the Top Ten list is Luis Macedo, a Latin Kings street gang member from Chicago wanted for the murder of a 15-year-old boy in 2009. Macedo led a group of gang members who beat the victim with a baseball bat, shot him, and then set his body on fire.

Twenty-one years old when the murder occurred, Macedo had already been an active gang member since he was a young teen and was in charge of the street crew that set upon the 15-year-old, who was not a rival gang member but was in the neighborhood visiting his girlfriend.

"The murder was classic mob mentality," said Patrick Johnson, a Chicago Police Department detective who is a member of the FBI's Violent Crimes Task Force in Chicago and who has been working to locate Macedo.

In the weeks after the killing, Macedo and four of his accomplices were identified. The other four gang members were arrested and were either convicted at trial or pleaded guilty to the crime and are serving prison sentences. Macedo remains a fugitive.

"Over the years, we've had unconfirmed reports about him being in Florida and possibly in Mexico," Johnson said. "He also has family in Wisconsin and



Luis Macedo

Philip Patrick Policarpio

Indiana, but the trail has gone cold. We are hoping this substantial reward announced today will bring someone forward."

Special Agent Scott Garriola, a member of the FBI's Los Angeles Fugitives Task Force who has investigated numerous Top Ten cases, believes the reward—up to \$100,000 for information leading directly to an arrest—may also play a significant role in the Philip Patrick Policarpio case. "The money can be a strong motivating factor," he said, "and why would anyone want to protect him, considering what he did."

At a gathering of friends and associates, Policarpio got into an argument with his girlfriend who was 17 weeks pregnant. "In front of everyone," Garriola said, he began to beat her with his fists, then pulled a gun and shot her in the head, killing her instantly.

A known drug user, Policarpio fled and may have traveled to Las Vegas or possibly the Philippines, where he has family ties. "His pattern

is one of violence," said Garriola, "and he is always armed. He is the definition of a continuing threat to the community."

We need your help. If you have any information regarding Policarpio or Macedo, please contact your local FBI office, the nearest U.S. Embassy or Consulate, or submit a tip on our website. Both men should be considered armed and extremely dangerous.

Macedo and Policarpio are the 507th and 508th individuals to be named to the FBI's Ten Most Wanted Fugitives list. Since its creation in 1950, 475 of the fugitives named to the list have been apprehended or located—157 of them as a result of citizen cooperation.

Note: Philip Patrick Policarpio was taken into custody on May 29, 2016. Luis Macedo may have been located since this information was posted on our website. Please check www.fbi.gov/wanted for up-to-date information.

Help Us Find Them

National Missing Children's Day 2016

Earlier this year, two young kidnap victims from Washington State were safely recovered in Mexico after an investigation involving the FBI, local law enforcement partners, and Mexican authorities.

Fortunately, their story had a happy ending. Unfortunately, there are still many children in the U.S. whose whereabouts are unknown. So as we approach this year's National Missing Children's Day on May 25, the FBI would like to ask the public for its help in locating any of the victims pictured above from our Kidnapping and Missing Persons webpage.

With its partners, the FBI continues its efforts to eradicate

predators from communities and to keep children safe. Ready response teams are stationed across the country to quickly respond to abductions. The Bureau offers a full array of forensic tools such as DNA, trace evidence, impression evidence, and digital forensics. And through improved communications, law enforcement also has the ability to quickly share information with partners throughout the world.

The FBI has several programs in place to educate both parents and children about the dangers posed by predators—in person and online—and to recover missing and endangered children should they be taken. Through

our Child Abduction Rapid Deployment Teams, Innocence Lost National Initiative, Innocent Images National Initiative, annual Operation Cross Country operation, Office for Victim Assistance, Child Exploitation Task Forces, and numerous community outreach initiatives, the Bureau and all of law enforcement continue to place a premium on keeping the most vulnerable among us safe and secure.

Note: The children pictured here may have been located since this information was posted on our website. Please check www.fbi.gov/ wanted for up-to-date information.



Child Sex Tourism

Alaska Man Receives Prison Term for Crimes Committed in Cambodia

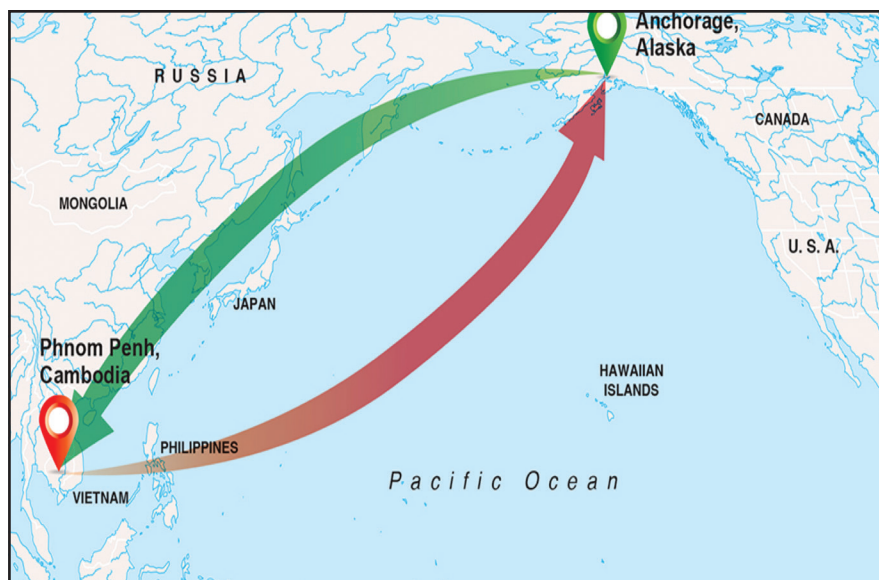
A tip to police from a concerned citizen in Anchorage, Alaska led to an FBI investigation that stopped a sexual predator from victimizing children in Cambodia—and landed the offender behind bars for a lengthy sentence.

In March, a federal judge sent 45-year-old Jason Jayavarman to prison for 18 years for attempting to sexually exploit children in Cambodia over a period of years and attempting to arrange a child sex tourism trip there for himself and others.

Jayavarman's crimes were "horrific," said Special Agent Jolene Goeden, who investigated the case from the FBI's Anchorage Division. In 2012, the Bureau was contacted by the Anchorage Police Department after a Crime Stoppers tip alerted the police to the possibility that Jayavarman was making frequent trips to his native Cambodia to have sex with children—an illegal act.

A preliminary investigation revealed that Jayavarman, who owned and operated a popular youth hostel in Anchorage and who has dual citizenship in the U.S. and Cambodia, had made at least a dozen such trips between 2010 and his arrest in 2013. During that time, it was later learned, he produced videos of himself having sex with a child victim.

As part of the investigation, an undercover source posed as a man interested in a child sex tourism trip. Over a period of months, Jayavarman "talked very openly about production of child pornography in Cambodia, how to smuggle that pornography back into the U.S., and about his connections in Cambodia and how he could procure young children for



Alaska resident Jason Jayavarman was sentenced to 18 years in prison for attempting to sexually exploit children in Cambodia over a period of years and attempting to arrange a child sex tourism trip there for himself and others.

his friends—some as young as 12 years old," Goeden said.

Jayavarman was arrested before he could travel overseas again, "but he had purchased his tickets along with those of the undercover source he believed would be accompanying him," Goeden noted.

A search of Jayavarman's house revealed child pornography, and from that evidence, investigators were able to identify one of the child victims in Cambodia. "We tracked her down in a mountain village in the middle of nowhere," Goeden explained, "and we were able to interview her."

Investigators learned that the victim was 14 years old when Jayavarman first began sexually abusing her. A year later he began making pornographic videos with her and ultimately recorded more than eight hours of him having sex with the girl.

After his arrest, Goeden said, Jayavarman discussed how it was common for extremely poor, young

Vietnamese and Cambodian girls to be traded to traffickers by their families for food. Many are brought from their rural villages to the Cambodian capital, Phnom Penh, which is where Jayavarman had first met the young victim.

"He was definitely a predator," Goeden said. During recorded conversations with the undercover source, "Jayavarman went on in detail about how to groom a child and what to do to a child," she said. "It was incredibly graphic and very disturbing."

Child sex tourism is a serious crime, Goeden added, "and it happens more than we realize. Some people think that what they do overseas can stay overseas, but that is not the case. The FBI is serious about stopping those who sexually exploit children, no matter where the crimes are committed."

Civil Rights and Law Enforcement

Director Speaks at Birmingham Conference



FBI Director James Comey speaks at the annual FBI and Birmingham Civil Rights Institute conference on law enforcement and civil rights.

It was September 15, 1963 when a bomb exploded inside the 16th Street Baptist Church in Birmingham, Alabama, killing four young girls and injuring countless others before Sunday worship.

The racially charged attack at the African-American church drew national attention and marked a major turning point in the civil rights movement. It was this act of violence and numerous other atrocities that ultimately led to the passage of the landmark Civil Rights Act of 1964, which provided the FBI with new federal laws to investigate civil rights violations.

Decades later, on the hallowed ground of the historic church, FBI Director James B. Comey recalled the discrimination African-Americans in Birmingham have faced during a speech today at the annual FBI and Birmingham Civil Rights Institute (BCRI) conference on law enforcement and civil rights.

“Too many have forgotten what it was like for men and women of color—for black people—in this city 50 years ago. But many of you here today remember, because many of you and your relatives lived it. Separate schools. Separate neighborhoods. Separate lives,” said Comey. “You fought against racism and inequality and the tremendous inertia of the status quo.”

Comey’s speech ended the two-day conference, which focused on the need to bridge the gap between law enforcement and the community, particularly in communities of color. As violent crimes increase in many parts of the country—including Birmingham, where 2015 brought on 88 homicides—Comey discussed how the lines between citizens and police are moving further apart. To change this trend, the FBI Director stressed the importance of developing a deeper understanding and a stronger connection.

“It is hard to hate up close,” Comey said. “It is hard to hate someone you know, someone whose life you have come to understand. And only by getting close to each other can we begin to arc those lines back together.”

Comey outlined several strategies to improve communication between the community and law enforcement, calling for better transparency, accountability, and partnerships. Birmingham, he said, is a good example of how the FBI works side-by-side with municipal organizations to stem violent crime.

For decades, the FBI’s Birmingham Field Office has worked closely with partner agencies on task forces to investigate cases, protect citizens, and train fellow law enforcement officials.

“The FBI has been a vital partner here in Birmingham,” said Don Lupo, director of citizen assistance for the Birmingham mayor’s office. “The local field office has been



FBI Director James Comey joins his wife Patrice for a tour of the Birmingham Civil Rights Institute museum on May 25, 2016 in Birmingham, Alabama. Comey provided remarks earlier in the day on civil rights and law enforcement at the historic 16th Street Baptist Church across the street.

completely supportive of everything that we have attempted to do in the city. The strong working relationship between our police and sheriff's department has been vital to the protection of our citizens."

Along with its enterprise with the city police, the FBI has partnered since 2006 with BCRI to educate law enforcement officials and the community on the history of the civil rights movement as well as current issues impacting neighborhoods across the country. Through the FBI and BCRI's annual conferences, the two agencies have built upon previous years' discussions to maintain an open dialogue between law enforcement agencies, their personnel, and the communities they serve.

"We believe that these conferences build ongoing and lasting relationships," said Priscilla Hancock Cooper, BCRI's vice president of institutional programs.

"Not only do we want to continue to engage law enforcement and community members in Birmingham, but I think we have something to offer to the rest of the country. Through our relationship with the FBI, we'll look for ways to spread this effective law enforcement partnership with other cities."

As Comey concluded his speech in front of a packed crowd at the historic Baptist church, he recalled the stories of every day people living in Birmingham during the civil rights movement who risked their lives to take a stand for racial equality—people like Bishop Calvin Woods, sitting in the audience today, who was determined to speak out against segregation despite being sentenced to hard labor.

"He said he kept marching, kept peacefully protesting because of his fellow citizens," Comey said. "Because despite the beatings, the

jailings, and the bombings, the spirit and determination of the black people of Birmingham could not be destroyed."

As the FBI continues to root out hate crimes and color of law violations and protect civil rights, Comey stressed the importance of citizens and law enforcement working together.

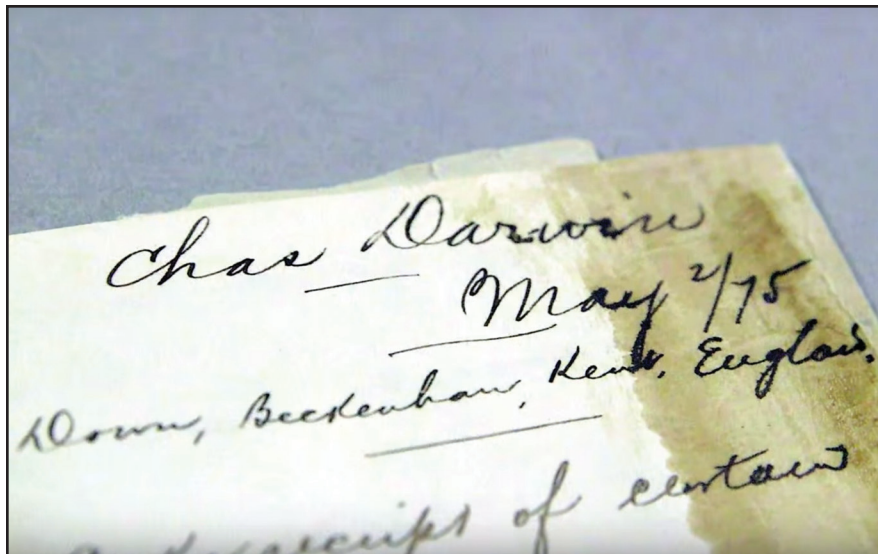
"It will take all of us—every single member of every community—to fight for and deliver change. To fight for equality and fairness. To stop driving around the problem. To be agitators and insiders, in the best way—in the way Dr. King taught us," said Comey.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/comeybirmingham.

Darwin Letter Recovered

FBI Returns 1875 Correspondence to Smithsonian Archives



A handwritten letter by Charles Darwin that was stolen from the Smithsonian Institution Archives more than three decades ago was recovered by FBI special agents and returned last week to the care of the Smithsonian.

The letter, written in 1875 by the British naturalist and geologist best known for his theory of evolution, was stolen in the mid-1970s from a collection of correspondence and documents relating to the history of North American geology. The FBI received a tip about the letter earlier this year, and special agents on the Bureau's Art Crime Team recovered the artifact. There are no criminal charges pending in the case because the statute of limitations has expired.

"Thanks to a tip from a member of the public, we were able to return this artifact to the care of the Smithsonian Archives," said Paul Abbate, assistant director in charge of the FBI's Washington Field Office. On May 26, he turned the letter over to Anne Van Camp, director of the Smithsonian Archives. "It's a privilege," Abbate said in a statement, "to return a piece of the history of science and exploration in the United States to

the American people."

The letter, written to American geologist Ferdinand Vandever Hayden, was part of the George Perkins Merrill Papers. Merrill was head curator of the Department of Geology in the early 1900s at what is now the National Museum of Natural History in Washington, D.C. Smithsonian conservators worked closely with FBI art crime experts to authenticate the Darwin letter, which went missing before it was cataloged in the Smithsonian Archives. Smithsonian experts were able to compare the letter to another one in their collection that Darwin wrote to Hayden.

"This is an important event, as this type of crime is not easily detected, and it demonstrates how seriously the FBI regards our cultural heritage," Van Camp said. The fact that the recovered letter is dated—May 2, 1875—adds a measure of context and value to the collection, Smithsonian officials said.

In the letter, Charles Darwin wrote to Hayden to thank him for sending two geological field studies of the American West, including the region that became Yellowstone National Park.

The text of the letter reads as follows:

May 2nd

Dear Sir,

I am much obliged to you for your kindness & for the honour which you have done me in sending your Geological Report of the Yellowstone River & your Preliminary Field Report on the Colorado & New Mexico. I had heard of your Geological researches on the Colorado & was anxious to see the conclusions at which you had arrived, & I am therefore especially obliged to you for having sent me your works.

With much respect & my best thanks, I remain,

Dear Sir,

yours faithfully

Charles Darwin

FBI Special Agent Martin Licciardo was a supervisor on the case and worked closely with Art Crime Team agents, who are trained in art and cultural property crime investigations. Members of the team are assigned to geographic areas around the country, including one at the Washington Field Office.

"The fact that we're able to take a piece of history that's so valuable to our generation and the fact that it can be on display for future generations to enjoy in the hands of its rightful owner—and not in some location where it shouldn't have been—it's pretty amazing," Licciardo said.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/darwinletter.

Oil and Crime in Indian Country

Director Visits Reservation in North Dakota to Discuss Rising Threat

Since 2008, a remote Indian reservation in northwest North Dakota has seen an explosive increase in crime following a now-waning oil boom in the region.

But while oil drilling and production has slowed in Fort Berthold, illegal activity like drug and human trafficking, prostitution, domestic abuse, and homicides are still on the rise. And limited resources have strained the ability of tribal police and the sheriff's department to respond quickly to incidents that have been occurring across six different counties in the area.

"We've been struggling with an increase in crime at Fort Berthold over the last seven or eight years, and we're actually getting a little bit desperate," said Mark Fox, tribal chairman of the Mandan, Hidatsa, and Arikara (MHA) Nation on the reservation. "The illegal activity here is literally killing our people and tearing us apart."

Standing by the Bureau's commitment to protect communities like the MHA Nation throughout Indian Country, FBI Director James Comey met with tribal officials, congressional leaders, and local law enforcement personnel yesterday in New Town, North Dakota to discuss the myriad challenges facing the reservation.

Later that day, Comey helped celebrate the opening of a new FBI resident agency in Williston, North Dakota, the result of collaborative efforts by North Dakota officials to gain additional Bureau support. Comey said three special agents and support staff assigned to the office will allow other FBI resources to point their efforts toward Fort Berthold.



FBI Director James B. Comey joins Mandan, Hidatsa, and Arikara Nation Tribal Chairman Mark Fox for an aerial tour of Fort Berthold Indian Reservation in northwestern North Dakota on June 6, 2016. During the tour, Fox described how the communities and landscape below have been impacted by the sharp influx in oil drilling since 2008. The tour was part of Comey's visit to the reservation, where he met with state, local, and tribal leaders to discuss the Bureau's support in fighting rising crime caused by the oil boom.

"The opening of our office in Williston should have a real-life impact on Fort Berthold," Comey said. "We're going to look at what effect that has on the resources we already have and think about what more we could do."

The opening of the new office comes at a time when FBI agents and other personnel stationed at Bureau's Minot Resident Agency were traveling between Williston and Fort Berthold to investigate crimes and assist partner law enforcement agencies. Comey said additional resources will provide a greater sense of relief and allow staff to spend more time in the region.

"The significance of the work Director Comey has done to establish an FBI presence in Williston is absolutely remarkable," said North Dakota U.S. Attorney Christopher Myers. "The presence of the FBI in the Bakken has tripled since the push has been

made to get more FBI resources, which is a great thing."

All of the officials at the New Town meeting, including Comey, agree that there is more work to be done to stem the flow of crime on the Fort Berthold Indian Reservation, and measures are already being considered to strengthen partnerships.

With the opening of the new Williston office and the discussions during this week's visit, Comey said he is considering the reinvigoration of an FBI Safe Trails Task Force, which existed in the area years ago.

Currently, there are 15 Safe Trails Task Forces operating throughout the United States. Their purpose is to unite the Bureau with other federal, state, local, and tribal law enforcement agencies in a collaborative effort to combat crime in Indian Country, especially violent crime, drug crime, gangs, and gaming violations.

Animal Rights Extremists

Pair Took Law into Their Own Hands



On an August night in 2013, a family-owned mink farm in Morris, Illinois came under attack. Approximately 2,000 minks were released from their cages, an acidic substance was poured over two trucks parked on the property, and a sign spray-painted on the barn declared, "Liberation is Love."

Some 24 hours later, when a police officer from nearby Roanoke, Illinois pulled over a car without license plates, he had no idea that the two young men inside were responsible for the earlier crime.

When the men's stories didn't add up about why they were driving a vehicle with no license plates or temporary tags, or what they were doing late at night on that deserted, rural road, the officer became suspicious. A search of the trunk revealed some curious items: books about terrorism and surveillance techniques, ski masks, and bolt cutters. The pair also had police scanners in the car, manually programmed to receive the frequencies of local police departments.

Kevin Johnson and Tyler Lang, both from California, were taken into custody for possessing burglary tools, and when it was later learned that the men were animal rights activists, the local authorities alerted the FBI.

"These two individuals were known animal rights extremists," said Special Agent Maureen Mazzola, who specializes in domestic terrorism matters and investigated the case from the FBI's Chicago Division. "We also knew they were based in California. The fact that they were pulled over in Illinois, 90 miles from the mink release that occurred the previous night, and that they were only a few miles away from a fox farm," she added, "was too much of a coincidence."

The subsequent investigation resulted in the pair being federally indicted in 2014 for damaging and interfering with the mink farm operations and conspiring to do the same thing to the Roanoke fox farm. Two other individuals—friends of Johnson and Lang—have been charged in connection with a spree of similar incidents in the summer of 2013. Joseph Buddenberg and Nicole Kissane are accused of terrorizing the fur industry, causing hundreds of thousands of dollars in damages by freeing minks and destroying breeding records in Idaho, Iowa, Minnesota, Wisconsin, and Pennsylvania.

Mazzola noted that most animal rights advocates don't believe criminal activity is the way to obtain their goals. But for those

Left: When a family-owned mink farm in Illinois was attacked by animal rights extremists in 2013, 2,000 minks were released from their cages and a barn was spray-painted with the words "Liberation is Love."

few in the movement who support extremist ideology, "they feel that the only way to deal with companies and people involved in what they perceive as animal cruelty is to hit them with some type of criminal act," she said. "They believe that legal protests are not enough and will never be enough."

As a result of such crimes, in 2006 Congress passed the Animal Enterprise Terrorism Act, strengthening an existing statute and allowing the Department of Justice greater authority to target animal rights extremists. The law also offers more protections to those involved in animal research or who work in the animal industry—the usual victims of animal rights extremists.

Last year, Johnson, 28, pled guilty to the charges against him and was sentenced in February 2016 to three years in prison. Lang, 27, who also pled guilty last year, was sentenced in March to six months of home confinement. In February 2016, Buddenberg and Kissane both pled guilty in San Diego federal court to conspiracy to violate the Animal Enterprise Terrorism Act. They are awaiting sentencing.

The owners of the Illinois mink farm, meanwhile, lost everything when their farm was vandalized, and many of the minks died. "The farm was the primary source of the owner's retirement and was how he supported his family," Mazzola said. "Everything they had was tied up in the business."

Director Provides Update on Orlando Shootings Investigation



FBI Director James Comey—joined by Deputy Attorney General Sally Yates—addresses members of the media during a press briefing held June 13, 2016 at FBI Headquarters regarding the recent mass shooting at nightclub in Orlando, Florida.

FBI Director James B. Comey said today that the FBI is working non-stop to understand what led a man to commit a mass shooting in Orlando, Florida that left 49 people dead and dozens more injured.

In a televised news briefing at FBI Headquarters, Comey said FBI investigators—working closely with state and local law enforcement agencies—are trying to understand “every moment of the killer’s path” leading up to the shooting early Sunday morning at a popular nightclub.

Comey said the shooter, who was killed in a gunfight with police responders, made three 911 phone calls from the club during the attack, beginning at about 2:30 a.m. In the calls, he claimed allegiance to the leader of the so-called Islamic State (ISIL) as well as the perpetrators of the 2013 Boston Marathon attack and a Florida man who died as a suicide bomber in Syria for a terrorist group in conflict with ISIL.

“There are strong indications of radicalization by this killer and

of potential inspiration by foreign terrorism organizations,” Comey said, adding that the FBI is the lead investigative agency on this case because it is a terrorism investigation.

Director Comey also described the FBI’s prior contacts with the killer, beginning in May 2013. The FBI opened an investigation when the shooter, then working as a contract security guard, made some inflammatory comments to co-workers and claimed a family connection to al Qaeda. The shooter was interviewed twice during the preliminary investigation, where he admitted making the statements but said he had done so in anger at his co-workers, who he believed were discriminating against him. The case was closed after 10 months.

Two months later, the shooter’s name surfaced as a casual acquaintance of the Florida man who blew himself up in Syria for the terrorist group al Nusra Front. “Our investigation turned up no ties of any consequence between the two of them,” Comey said. “We

will continue to look forward in this investigation, and backward. We will leave no stone unturned.”

Comey said the Bureau is reviewing those cases to see if anything was missed. “We’re also going to look hard at our own work to see whether there is something we should have done differently. So far, the honest answer is: I don’t think so. I don’t see anything in reviewing our own work that our agents should have done differently.”

The Director, who was joined at the press briefing by Deputy Attorney General Sally Yates, expressed sorrow for the victims and their families.

“Our hearts are broken and ache for the people who are lost in Orlando, those wounded, and their families,” he said.

Comey also thanked first responders for their heroic work. “They showed professionalism and extraordinary bravery that saved lives,” he said. “We are very lucky that such good people choose lives of service in law enforcement.”

Cold Case Killer

Help Us Catch the East Area Rapist

The FBI and its law enforcement partners are seeking the public's assistance with information about an unknown individual known as the East Area Rapist/Golden State Killer (EAR/GSK). Between 1976 and 1986, this individual was responsible for approximately 45 rapes, 12 homicides, and multiple residential burglaries throughout the state of California.

Although four decades have passed since a prolific serial rapist and murderer terrorized California communities from Sacramento to Orange County, the FBI and

leading to the arrest and conviction of the killer along with a nationwide multimedia campaign to once again bring the case to the public's attention.

"Regardless of the amount of time that has passed," said Sgt. Paul Belli, the Sacramento County Sheriff's Department detective assigned to the case, "the sheriff's department never gave up on the investigation. This person ruined a great number of lives, and he should be held accountable."

During the time he was operating in Sacramento, between 1976

law enforcement techniques, and he was proficient with firearms.

Detectives have DNA from multiple crime scenes that can positively link—or eliminate—suspects. This will allow investigators to easily rule out innocent parties with a simple, non-invasive DNA test.

"Just like any homicide investigation," Belli said, "our lifelines are people who give us information. It all boils down to people helping." He added that the \$50,000 reward could motivate someone to come forward. "It may

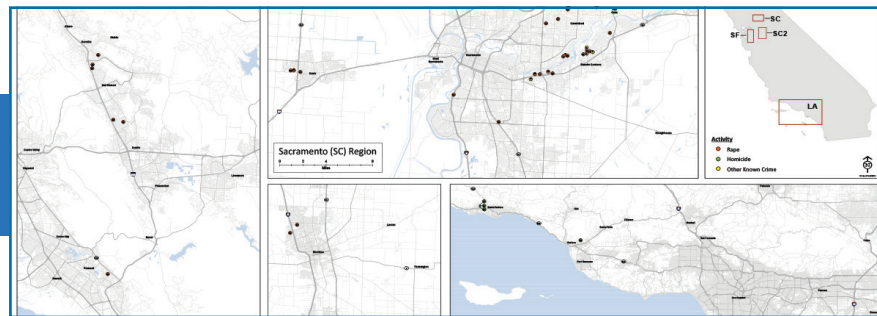


Investigator looks at crime scene photos

local law enforcement announced a national publicity campaign today—and a significant reward—in the hopes of locating the suspect and finally bringing him to justice.

Between 1976 and 1986, the violent and elusive individual known as the East Area Rapist, and later as the Original Night Stalker and the Golden State Killer, committed 12 homicides, 45 rapes, and more than 120 residential burglaries in multiple California communities. His victims ranged in age from 13 to 41 and included women home alone, women at home with their children, and husbands and wives.

At a press conference today in Sacramento, the FBI and local law enforcement agencies announced a \$50,000 reward for information



Map showing locations of attacks by region of the East Area Rapist in California

and 1978, the East Area Rapist struck fear and anxiety into the community. "Everyone was afraid," said Special Agent Marcus Knutson, who was born and raised in Sacramento and now heads the FBI's portion of the investigation. "We had people sleeping with shotguns, we had people purchasing dogs. People were concerned, and they had a right to be. This guy was terrorizing the community. He did horrible things."

If he is still alive, the killer would now be approximately 60 to 75 years old. He is described as a white male, close to six feet tall, with blond or light brown hair and an athletic build. He may have an interest or training in military or

push somebody over the edge who knows something. It could provide us with that one tip we need."

Investigators are urging the public to provide law enforcement with any information, no matter how insignificant it may seem. If someone knows a person in the right age range who lived in the area at the time and who seemed suspicious or who may have had some involvement, "we can determine where they are living," Belli said. For those who come forward, he added, "we are very discreet about privacy and confidentiality."

It is known that the East Area Rapist took things from crime scenes—coins and jewelry in particular. The public is asked to

be mindful of that. “We know that our guy took items,” Knutson said. “So if for some reason people—whether their family member is deceased or they’re cleaning out a storage unit—come across a weird collection of items such as women’s ID’s, rings, earrings—anything that’s out of the ordinary—it could be significant.”

In addition to supplying the reward money, the FBI is assisting local investigators by following leads all over the country, Knutson said, ruling out suspects based on DNA tests and other evidence. When

Ray Biondi, a retired Sacramento County Sheriff’s Department detective, investigated the double homicide, which was quickly linked to the East Area Rapist. “This threw a whole different light on the rape series,” said Biondi, who spent 17 years as a homicide detective and investigated hundreds of murders.

One of his few regrets about retirement, Biondi said recently, “was leaving the cases I didn’t solve.” What strikes him about the Maggiore murders and the East Area Rapist is how the subject has

18-year-old woman was raped and murdered in Irvine, California—the last known crime associated with the subject.

Knutson, too, believes that capturing the East Area Rapist is still possible. “Sometimes it’s just one call that makes a difference,” he said. “If we get that one call and we are able to compare DNA and say, ‘Yes, it’s him,’ then we have him. But it starts with that one call, and that’s why we are seeking the public’s assistance.”

Being a Sacramento native makes this case even more meaningful for



Sketches of the suspect



Crime scene photo

the crimes were committed, DNA testing was not available, nor was other technology such as cell phones, neighborhood surveillance cameras, or, in many areas, the 911 emergency call system.

Burglaries and rapes began occurring in the eastern district of Sacramento County—hence the name East Area Rapist—in the summer of 1976. The subject ransacked homes and took coins, jewelry, and identification. Neighborhood burglaries were often followed by clusters of sexual assaults. Then, on February 2, 1978, Brian Maggiore and his wife, Katie, were on an evening walk with their dog in their Rancho Cordova neighborhood when they were chased down and murdered.

managed to elude capture. “It is mind-boggling that he committed so many crimes without a slip up,” the veteran detective said. And yet, one of Biondi’s first homicide cases decades ago was recently solved through DNA evidence. So it is entirely possible, he said, that the East Area Rapist can be brought to justice. “That would elate me.”

After his crimes in the Sacramento area, the subject continued primarily in the East Bay Area of Northern California, where his activity escalated into rapes and homicides along the California coast. He would attack couples, tie up both victims, rape the female, and then murder them. After July 1981, no associated incidents are known until 1986, when an

Knutson. “This is my home,” he said. “This is where I’m from. The fact that he did his crimes here I take personally, and I’m proud that I’m able to work with the local sheriffs’ offices to investigate this case and try to get this guy in custody.”

We need your help. Individuals with information are urged to call 1-800-CALL-FBI (1-800-225-5324). Information may also be submitted online at tips.fbi.gov.

Note: This case may have been resolved since this information was posted on our website. Please check [www.fbi.gov](https://www.fbi.gov/eastarearapist) for up-to-date information.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/eastarearapist.

Taking Flight

Man Sentenced for Distributing Avionics Trade Secrets



While Derek Wai Hung Tam Sing was employed at avionics firm Rogerson Kratos, he stole trade secrets related to his work on helicopter instrument systems and displays such as this; following his dismissal, he sent the proprietary information to the company's competitors.

For an aircraft electronics company looking to ramp up production, Derek Wai Hung Tam Sing must have seemed like a dream hire—20 years of experience as an electrical engineer and an extensive résumé.

But the Glendale, California resident turned out to be a nightmare for his employer, Rogerson Kratos.

Sing was hired by the Pasadena-based firm in April 2012 to improve avionics systems and circuit boards that would ultimately end up in military helicopters. Before starting work with the company, Rogerson Kratos required Sing to sign a confidentiality agreement prohibiting him from sharing trade secrets with anyone outside the company.

Despite the agreement, Sing stole and distributed product schematics to several competitors, violating the Economic Espionage Act. The crimes resulted in an investigation by the FBI, which ended up landing Sing in federal prison.

"The whole time Sing was at Rogerson Kratos, he was bringing

home a treasure trove of work files and project photos," said Special Agent Michael Fitzpatrick, who investigated the case out of the FBI's Los Angeles Field Office. "He never had permission to do that and wasn't following company protocols."

In the seven months that Sing was employed at the company, he often missed project deadlines, struggled with tardiness, pushed back on leadership decisions, and ridiculed fellow employees.

Sing's unprofessional behavior and poor work performance got him fired in November 2012. Disgruntled over the company's actions, he set on a vengeful mission—according to his testimony at trial, he "wanted to get back at Rogerson Kratos" for being unappreciative of his efforts.

"Harming Rogerson Kratos for what they did to him was a top priority for Sing," said Fitzpatrick. "He had the advantage of possessing their trade secrets and the means to distribute them widely to competitors."

In December 2012, Sing packaged up seven different product schematics along with files that explained the importance of the proprietary information and instructions on how to reverse-engineer the products. In early 2013, he used fictitious e-mail accounts to send the stolen trade secrets to domestic and foreign companies that produced avionics products.

One overseas recipient of Sing's communications realized the files contained stolen trade secrets, determined the information belonged to Rogerson Kratos, and alerted the company. In turn, Rogerson Kratos contacted authorities, which led to the FBI opening an investigation in February 2013. Through a series of search warrants, evidence-gathering, and interviews, agents found Sing to be the source of the leaked trade secrets.

"Rogerson Kratos would have faced millions of dollars in lost revenue if any of the companies that received Sing's files actually took advantage of them," said Fitzpatrick. "If it wasn't for the ethical decision-making of one organization, untold damage could have been committed."

Sing was arrested and indicted in April 2014 following the FBI investigation. In December 2015, he was convicted of 32 counts of violating the Economic Espionage Act by stealing trade secrets from his former employer. On June 6, 2016, the 45-year-old was sentenced to one year and one day in prison for his crimes.

Taken Hostage

Mexican Drug Cartel Influence Felt in Rural South Carolina

The crimes and violence associated with Mexican drug trafficking organizations can reach almost anywhere in the United States, as evidenced by a 2014 kidnapping in rural South Carolina that resulted in the convictions of three cartel-connected men—one of whom was recently sentenced to more than five decades in prison.

On the morning of July 9, 2014, in the small town of St. Matthews, South Carolina, 23-year-old Cory Still left home for his job as a roofer, but he never made it to work. His fiancée found his abandoned truck on the side of the road a few hours later with the keys still in it, and her family filed a missing person report with the Calhoun County Sheriff's Office. When the woman's cell phone rang that night, the caller informed her that Still was alive, that instructions would come in 24 hours, and that Still's father had better be there to answer the next call.

Still—who would later be charged and plead guilty to conspiracy to distribute marijuana—had been kidnapped because of his father's \$200,000 debt to the cartel over a missing drug shipment. The FBI was contacted the next morning, and what followed was an intense, six-day law enforcement effort that involved several FBI offices and hundreds of Bureau personnel from around the country, including crisis negotiators, linguists, SWAT, and the Hostage Rescue Team.

"We worked around the clock interviewing Still's family and associates to develop and run to ground every possible lead," said Special Agent Luke Davis, who is assigned to the FBI's Columbia Field Office. "Thanks to a crucial error made by one of the



kidnappers, within a few hours, we were able to identify a cell phone and track them to rural eastern North Carolina."

The first ransom call to Still's fiancée showed a number that originated from Mexico. Investigation revealed that minutes prior to that call, the caller had dialed a number with a 910 area code, which is in North Carolina.

Agents worked quickly to obtain a court order to monitor those phone numbers, which would eventually lead to Still and the arrest of three subjects. But during much of the time he was held hostage, the victim was blindfolded, threatened at gunpoint, bound with zip ties and rusty chains and padlocks, and made to lie on the floor for days.

At times during more than a dozen ransom calls, the kidnappers told Still's father he was going to find his son with his eyes cut out, Davis said. Other calls implied that if the money wasn't paid, "they were going to close the case," meaning Still would be killed. "There is no doubt in my mind that if we didn't find him, he would not be alive today," Davis added.

Based on the phone monitoring and subsequent physical surveillance, it was determined that the kidnappers might be holding Still in North Carolina.

In the early morning hours of July 15, 2014, six days after Still's abduction, operators with the FBI's Hostage Rescue Team executed a search warrant in Garland, North Carolina. One of the kidnappers, Juan Fuentes-Morales, was arrested. Agents recovered the cell phone they had been monitoring and a pistol used during the abduction—but Still was nowhere to be found.

A short time later, the FBI's Charlotte and Richmond SWAT teams executed another search warrant near Roseboro, North Carolina, where they found Still blindfolded and chained to a workout bench on the floor. The other two kidnappers, Ruben Ceja-Rangel and Luis Castro-Villeda, were arrested at the scene.

In 2015, Castro-Villeda pled guilty to kidnapping and other charges and was sentenced to 30 years in prison. Last month, a federal judge sentenced Ceja-Rangel to a prison term of 56 years. Fuentes-Morales has yet to be sentenced.

Davis credits his dedicated FBI colleagues and local law enforcement personnel for Still's safe return and for taking three violent criminals off the streets. Did it surprise him that Mexican drug cartels had made it to small-town South Carolina? "Not at all," he said. "The traffickers are everywhere."

Intellectual Property Crime

Trio Pirated Mercedes-Benz Diagnostic Software



Left: Three men who produced, marketed, and sold non-authentic Mercedes-Benz diagnostic software systems such as this were sentenced for their roles in the intellectual property crime.

The case of the pirated Mercedes-Benz software is a classic example of how a company's intellectual property can be compromised—and how criminals can profit from someone else's hard work.

In April 2016, California resident Martin Vellozzi was the last of three individuals sentenced for creating and selling non-authentic Mercedes-Benz diagnostic software systems. The diagnostic systems are used by auto mechanics to diagnose and fix Mercedes vehicles. For more than a decade, Vellozzi and his co-conspirators—Rainer Wittich of Louisiana and Robert Beckmann of North Carolina—made money by stealing the proprietary software and selling it at a steep discount.

"All three conspirators had legitimate businesses in the automotive industry," said Special Agent Sundanah Parsons, who investigated the case from the FBI's New Orleans Field Office. "Each one had a different kind of expertise, and they came together to profit from their illegal activity."

The Mercedes-Benz Star Diagnostic System is a hand-held computer containing proprietary, confidential software that costs as much as \$22,000. "Vellozzi discovered a way to pirate the

software from legitimate Star Diagnostics Systems," Parsons explained, "which over the years effectively robbed Mercedes of millions of dollars in business opportunities."

By stealing the Mercedes software—and without having to spend money on research and development—Vellozzi, Wittich, and Beckmann were able to produce, market, and sell their illegal versions of the system on laptop computers for anywhere from \$6,000 to \$12,000. Court records indicate the trio sold nearly 1,000 of the units. "They were selling them all over the country and even internationally," Parsons said. "It was all about the money."

In 2011, representatives from Mercedes-Benz contacted the FBI's Intellectual Property Rights Unit to report their suspicions that the diagnostic system had been compromised. The Bureau later sent an undercover operative to one of Vellozzi's automotive repair seminars, where the pirated units were being openly sold.

"Mercedes was rightfully concerned about its intellectual property," Parsons said, explaining that the diagnostic system could be used to modify and control a variety of critical features on automobiles,

including air bags and braking systems.

"Vellozzi and his colleagues knew what they were doing was illegal," Parsons added. "Although the units were being sold openly at seminars he held around the country, Vellozzi didn't advertise the systems on his website or list them anywhere in his business records—and neither did Wittich and Beckmann."

In April, a federal judge sentenced Vellozzi to four years' probation and a \$6,000 fine. In January 2016, Wittich and his Louisiana-based aftermarket auto parts distributor business, The Brinson Company, were sentenced for their roles after previously pleading guilty to criminal copyright infringement and violating the Digital Millennium Copyright Act. Wittich received five years of probation, and his company was ordered to forfeit \$150,000 and assist Daimler AG—parent company of Mercedes-Benz—in compiling a list of all customers to whom it provided the pirated software systems.

In March 2016, a federal judge sentenced Beckmann to four years of probation, with the first four months to be served on home detention, and a fine of \$5,000 for criminal copyright infringement. His company, Beckmann Technologies, was also sentenced to five years of organization probation and fined \$75,000.

"They all knew what they were doing was wrong," Parsons said. "They made a lot of money, but then they got caught."

New Top Ten Fugitive

Help Us Catch a Murderer

A Wisconsin woman charged with killing a pregnant woman and her unborn child has been named to the FBI's Ten Most Wanted Fugitives list, and a reward of up to \$100,000 is being offered for information leading to her capture.

Shanika S. Minor is wanted for the March 2016 murder of her mother's neighbor in Milwaukee, a 23-year-old who was five days away from her due date. The shooting stemmed from an argument over loud music being played from the victim's residence.

"Apparently Minor believed that the victim had somehow disrespected her or her mother," said Special Agent Chad Piontek, who is investigating the case from the FBI's Milwaukee Field Office. "It is a fairly violent neighborhood," Piontek said. "Unfortunately, there is sometimes a street mentality about solving problems."

According to witnesses, on March 5, 2016, Minor instigated an argument with her mother's neighbor after Minor's mother had previously said the neighbor was playing loud music at an unreasonable hour. On the sidewalk outside the victim's residence, Minor brandished a handgun and challenged the neighbor—her former high school classmate—to fight. Minor's mother ran to the scene and implored her daughter not to hurt the pregnant woman.

Minor fired a round from her gun into the air, got in her car and left the scene. "Most people who witnessed the incident thought that was the end of it," Piontek said. But it was only the beginning.

Shortly before 3 a.m. the next morning, Minor returned to the neighborhood, gained access to



the duplex her mother and the neighbor rented, and confronted the woman by the rear door of her residence. Minor's mother again ran to the scene, this time positioning herself between her daughter and the neighbor, trying to keep the peace. Witnesses said Minor reached over her mother's shoulder and fired her gun, striking the woman in the chest. The victim retreated into her residence, where she died in front of her two children. The unborn child also died.

Minor, 24, fled and has not been seen since. She has reportedly told acquaintances that she would not turn herself in. Minor may have contact with people in Missouri, Mississippi, Texas, Tennessee, Ohio, and Georgia. Other than delivering newspapers, "there is no record she had any reliable employment," Piontek said. "I don't think she has a lot of resources on her own. Clearly, people have assisted her."

Minor might be receiving help from extended family members or a "network of friends," Piontek said, adding that "such help is criminal, and individuals could be charged with aiding and abetting a fugitive."

There is also a physical risk to anyone helping Minor. "The murder weapon was not recovered, and it is likely she is still armed," Piontek said. "She killed someone who was not a stranger to her—a family acquaintance." He added that the reward offer could motivate someone to come forward. "Our hope is that whoever is assisting her will find the potential reward more attractive than protecting a person wanted for first-degree murder."

Minor is described as 5 feet 6 inches tall, having a medium build, and weighing 165 pounds. She has black hair and brown eyes. She should be considered armed and extremely dangerous.

"This was a senseless crime," Piontek said, "and we believe Minor is capable of more violence. We need to capture her so that no one else is harmed."

Anyone with information concerning Minor should contact the nearest FBI office or local law enforcement agency, or submit a tip online. The FBI's Milwaukee Division can be reached by phone at (414) 276-4684.

Note: Shanika S. Minor was taken into custody on July 1, 2016.

Forensic Anthropology

Laboratory Artist Puts a Human Face on Unidentified Remains



Left: Lisa Bailey, a forensic artist at the FBI Laboratory in Quantico, Virginia, creates facial approximations of unidentified individuals using models of their skulls and anthropologist reports.

Fifteen years ago, hikers in a suburban Minnesota park discovered the skeletal, unclothed remains of a woman, 35 to 45 years old, with brown or reddish hair and evidence of significant dental work. The woman was never identified, and the case remains open as a homicide investigation.

In a bid to develop fresh leads, police in New Brighton, Minnesota earlier this year circulated new images showing what the woman may have looked like when she was alive. The facial approximation—rendered in clay using a forensic analysis of the woman's skull, along with a detailed anthropological workup and a deft artistic hand—was aimed at putting a distinctive face in front of as many people as possible, raising the odds that someone will recognize her. The process is a free service provided by the Trace Evidence Unit at the FBI Laboratory in Quantico, Virginia to support the law enforcement community.

"This process has given me new hope that my unidentified person will be identified someday," said Mike Lochen, a detective in

the Police Division of the New Brighton Department of Public Safety.

Nationwide, about 4,400 unidentified remains are found each year—and more than 1,000 of those are still unidentified a year later, according to the National Institute of Justice, which maintains searchable databases of missing and unidentified persons (NamUs.gov). Medical examiners and local police departments most frequently become the stewards of unidentified remains. And each year, about 20 requests are made to the FBI Laboratory to develop facial approximations of unidentified individuals to help investigators ultimately put a name to a face.

In recent years, the Office of the Chief Medical Examiner in Virginia posted images of FBI facial approximations, hoping to generate leads. The ensuing media coverage led to three positive identifications. In Massachusetts, a woman was recently identified after her brother saw the approximation on the news.

"We need the right person to see this image pretty much at the right time," said Lisa Bailey, a visual information specialist at the FBI Lab who produces the Bureau's facial approximations in a collaborative effort that includes forensic anthropologists and technicians who extract as much data as they can from human remains. "That's one of the biggest things with these approximations—to get them out there. All we need is that one person to see it."

"You can't go too far and make it art. It can't be a portrait. You can't make it pretty. You have to pull back and only do what the skull is showing you."

What the public ultimately sees is the result of many hours of examination, preparation, and artistry. It all starts when remains arrive at the FBI Lab and anthropologists assemble a report based on what the remains reveal—the subject's age, sex, stature, and ancestry, for example. If there is a skull, a technician in the Lab's Operational Projects Unit digitally scans it to create an exact replica on a 3-D printer. By the time a case gets to Bailey, she has an anthropologist's report to refer to and a model skull on which to build her approximation.

"First, I read the anthropologist's report and I sit and just evaluate the skull," said Bailey, a graphic artist-turned forensic artist who joined the FBI 14 years ago.

She studies the face shape and proportions and looks specifically at features like the brow ridge, cheek bones, the set of the eyes, the aperture of the nose, and the alignment of teeth.

“Every face is different because every skull is different,” Bailey said. “You can recognize somebody—even at a distance—because of the proportion of their face.”

For ears, lips, and eyelids—which can’t be deduced from a skull—she refers to anthropological reference materials that include skull databases, catalogs of anonymous faces, and published research. The goal in an approximation is to draw attention to those prominent features revealed by the skull, and nothing else.

“That’s the hardest part about being a forensic artist,” Bailey said.

“You can’t go too far and make it art. It can’t be a portrait. You can’t make it pretty. You have to pull back and only do what the skull is showing you.”

When Bailey is finished, she reveals the sculpture to the anthropologist who made the initial assessment. Together they might make some adjustments to draw out specific features.

“I want to make sure what I see on that face is what I think corresponds to the skull,” said Dr. Richard M. Thomas, one of two staff anthropologists at the FBI Lab. “I try and make sure all those things are being brought out in the sculpture. I haven’t been working on it, so I’ll know exactly what I’m drawn to when I see the face.”

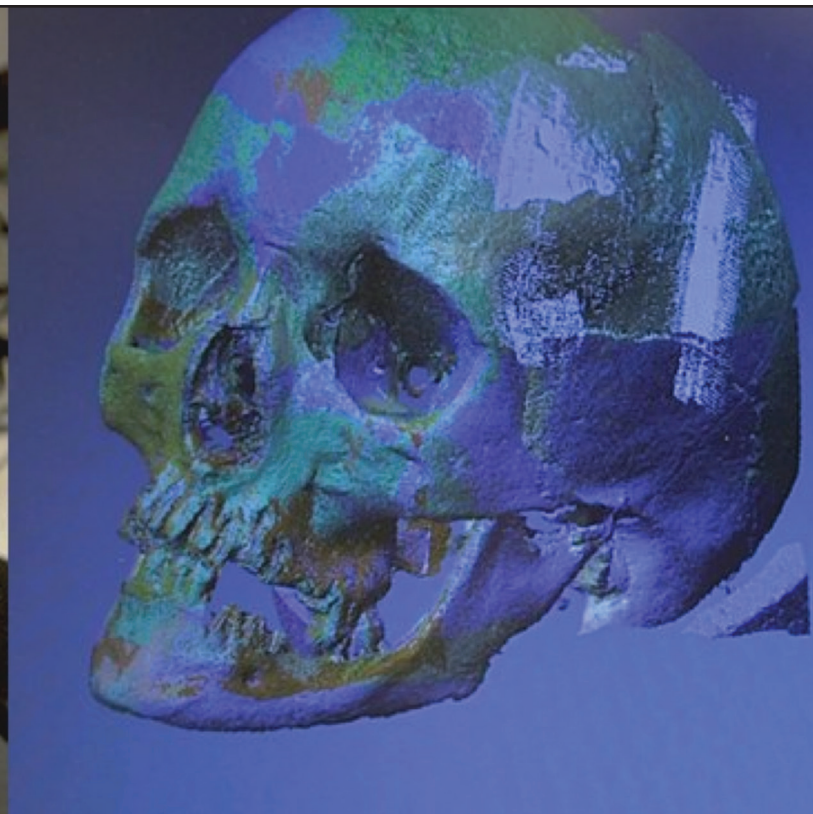
Investigators in Minnesota are hoping that moment of serendipity

is how someone will recognize the unidentified women found in 2000. Detective Lochen in New Brighton said the new approximation has developed a few leads, but no breakthroughs.

It just takes the right person looking at the right time to make a connection, Bailey said. Timing and luck. “Seeing that one image could be the thing that makes somebody take a second look.”



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/forensicanthropology.



The skulls of unidentified remains are digitally scanned and then replicated using a three-dimensional printer.

Electronics Smuggler Sentenced

Sensitive Equipment Illegally Exported to Russia



For more than six years, a New Jersey man who owned four microelectronics export companies skirted U.S. export laws enacted under the International Emergency Economic Powers Act (IEEPA). These laws are in place to help protect U.S. national security and make sure that items made in the U.S. don't help strengthen another country's military without proper licensing and careful consideration.

Alexander Brazhnikov, Jr., a 36-year-old naturalized American citizen born in Russia, admitted that, between January 2008 and June 2014, he smuggled \$65 million worth of sensitive electronics components from the U.S. to Russia, where much of it eventually ended up in the hands of Russia's Ministry of Defense and Federal Security Service.

In June 2015, Brazhnikov plead guilty in federal court—after a multiagency investigation by the FBI, the Department of Commerce, and Department of Homeland Security (DHS)—to the smuggling charges and to a charge of conspiring to commit money laundering to hide the illegal proceeds of his criminal activities. According to then-Newark FBI Special Agent in Charge Richard Frankel, Brazhnikov “significantly undermined the national security of the national security of the U.S.” and “enhanced the capabilities of both the Russian Military Service

and the Russian Nuclear Weapons Program.” Last month, he was sentenced to more than five years in prison.

Investigators believe that Brazhnikov conspired with his father, Alexander Brazhnikov, Sr., owner of a Moscow-based procurement firm who brokered the purchasing of electronics components from U.S. vendors and manufacturers for their clients, mostly Russian defense contractors licensed to procure parts for the Russian military, security service, and other entities involved in the design of nuclear weapons and tactical platforms.

The case began in 2012, when another Bureau field office—investigating a similar matter—sent a lead to the Newark FBI Office concerning one of Brazhnikov's companies. Joining forces with Commerce and DHS, investigators began looking into Brazhnikov and his New Jersey companies. Through a variety of investigative methods, including following the money trail, here's what they found:

Brazhnikov received requests for certain electronics components from co-conspirators in Russia. Funds for those components were deposited into Russian bank accounts, transferred to the offshore bank accounts of dozens of shell companies created specifically to facilitate the movement of the money and to hide its origin, and

then shifted to U.S. bank accounts controlled by Brazhnikov and his companies.

Using the money from these bank accounts, he would place orders for the electronics components he needed with U.S. manufacturers and vendors. But because of U.S. export laws, he knew that many of these components—having to do with areas like advanced communications, avionics, weapons testing, and encryption applications—would have been denied export to Russia's military and security services. So after receiving the components (often misleading the manufacturers and vendors about his intentions), he purchased and repackaged the goods for their journey to Russia. Brazhnikov also intentionally misled the shipping companies he dealt with by undervaluing the cost of what he was shipping and directing that the shipments be sent to front addresses in Russia—all in an effort to evade the legal requirements of obtaining the proper export permissions from the Department of Commerce.

Once the items were delivered in Russia, they were rerouted by members of the Moscow-based conspiracy to their true destination. Brazhnikov was responsible for more than 1,900 illegal shipments like this.

The FBI and its federal partners take safeguarding our national security very seriously—no matter what form those threats take—and we will continue to vigorously and lawfully investigate anyone whose criminal activities threaten that security.

Finding Solace

FBI Crisis Response Canines Help Victims Cope with Tragedy

After the mass terrorist shooting in San Bernardino, California, the FBI's Victim Assistance Rapid Deployment Team was among the first to respond.

The multidisciplinary group consisted of victim specialists, analysts, and special agents all trained in responding to mass casualty events.

While in San Bernardino, they connected grieving victims and their families to a variety of support services during the course of the investigation. But when it came to providing relief and comfort, the team relied on two English Labrador Retrievers for help.

Wally and Giovanni are the FBI's new crisis response canines. They are part of a pilot program recently launched by the Bureau's Office for Victim Assistance (OVA).

According to OVA Assistant Director Kathryn Turman, the dogs are an additional way her team can help victims and family members cope with the impact of crime.

"The Crisis Response Canine Program was a natural evolution in developing the Rapid Deployment Team's capacity," said Turman. "With San Bernardino and other places we've taken them, the dogs have worked a certain type of magic with people under a great deal of stress. That's been the greatest value."

Turman said the idea for the canine program stemmed from a conference she attended years ago in Canada, where she witnessed police victim service dogs in

action. Turman quickly brought the concept to life at the FBI when she returned home.

With help from the non-profit organization Assistance Dogs of the West (ADW), the FBI was matched with Wally and Gio in October 2015. Turman said ADW identified with the Bureau's victim assistance program, having trained dogs with a temperament for hospital and criminal settings. Their presence in courtrooms, for example, has helped ease stress in children giving testimony and aided prosecutors in achieving convictions.

"It's amazing how quickly Wally and Gio relax and disarm people," said Staci Beers, coordinator for the FBI Victim Assistance Rapid Deployment Team. "When we respond to a mass casualty event where emotions are high, their calming nature enable victims to engage with us and learn about the services we offer."

Beers and rapid deployment teammate Melody Tiddle both added dog handler to their list of victim assistance responsibilities when they traveled to San Bernadino in December 2015, after the shooting that claimed the lives of 14 people and left 22 seriously injured. The dogs joined Beers and Tiddle for hospital and family assistance center visits.

Wally and Gio were even requested by FBI staff and first responders at the incident command post.

"People at the command post were working long hours and were under a lot of pressure," said FBI Associate Deputy Director David Bowdich, who at the time was the assistant director in charge of the FBI's Los Angeles Field Office. "As the dogs roamed the area, I saw



Gio (above) and Wally (below) are the FBI's newest crisis response canines. The English Labrador Retrievers join the Victim Assistance Rapid Deployment Team in providing support to those affected by mass casualty events.



agents and task force members take time out to pet them. It was a good distraction."

Wally and Gio have been working steadily since returning from their first deployment. They deployed to Orlando in June following the mass shooting that claimed the lives of 49 people injured 53 others. And earlier this month they deployed to Dallas to help console victims and first responders following the mass shooting there that left five police officers dead.

"We are always looking for ways to make the unthinkable a little easier for people who experience it," said Turman. "The dogs have been a positive experience for us and one that I think has a very large benefit for the FBI."



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/crisisresponsecanines.

Background image: English Labrador Retrievers Wally (top) and Giovanni (bottom) are the newest members of the FBI's Victim Assistance Rapid Deployment Team.

The Long Hike to Prison

Fugitive Spent Years Hiding on the Appalachian Trail



In February 2009, James T. Hammes was called to his employer's headquarters in Cincinnati, Ohio to answer questions about a possible fraud scheme inside the company. A long-time, respected controller for a family-owned beverage bottling company, Hammes handled all his business division's vendor accounts and payments.

During the interview, conducted by the FBI, Hammes repeatedly denied any knowledge of the fraud. But shortly after he left the company's headquarters that day for his home in Lexington, Kentucky, the 46-year-old husband and father disappeared without a word.

Hammes was later charged with embezzling more than \$8.7 million from his employer over an 11-year period. "Agents recovered boxes of documents at his home that detailed the fraudulent transactions," said Special Agent Jonathan Jones, one of the investigators who worked the case from the FBI's Cincinnati Field Office. "It was also discovered that he was doing research on the Internet about how to disappear."

As it turns out, for the majority of his six years on the run, Hammes was hiding in plain sight on the Appalachian Trail, the nearly 2,200-mile wilderness path that

runs from Georgia to Maine. Hammes, who went by the trail name "Bismarck," came to be known and liked by fellow hikers on the trail. No one guessed his real identity or that he was wanted by the FBI.

Court documents show that Hammes' embezzlement began around 1998. As a controller, he was responsible for all financial accounting and internal controls for his division, including supervising accounts payable to several hundred outside vendors. He carried out the fraud by establishing a new bank account for an existing vendor at a different bank. He then deposited hefty payments to that vendor—often \$100,000 at a time—in the phantom account that he alone controlled. He then could transfer money from the phantom account to his personal accounts.

"He knew how to cover his tracks by manipulating audits and ledger entries," Jones said. "He got away with it for so long because he knew how to manipulate his subordinates and how not to raise accounting red flags."

Eventually, bank employees who handled accounts for the victim company and the vendor discovered canceled checks being returned from a bank they were unfamiliar with, and the scheme

began to unravel. Hammes was also coming under scrutiny from the Internal Revenue Service for failing to file tax returns. He had invested a majority of the stolen funds in the stock market and lost most of that when the market had a severe downturn in 2008.

While he was a fugitive, his wife divorced him. Hammes apparently had little contact with the outside world while he was hiking, so he may not have known that his case had attracted widespread media attention, including segments on popular crime reenactment shows such as *American Greed* and *America's Most Wanted*.

In late 2014, a hiker who had spent time with "Bismarck" on the trail was back at home when he happened to watch a rerun of *American Greed* that featured the Hammes case. He recognized his trail companion and called the FBI. Hammes was arrested in Virginia in May 2015 and pleaded guilty to wire fraud in connection with the embezzlement that October.

Jones credits the media and the public for assisting in the fugitive's capture. "Without the publicity," he said, "we may never have caught him." Last month, a federal judge sentenced Hammes to eight years in prison and ordered him to pay nearly \$8 million in restitution.

Jones pointed out that Hammes did not appear to have a gambling problem or a drug addiction, which often explains why people embezzle money. "I think he was just greedy," he said. "I think he just wanted a lifestyle that his current position couldn't afford him. He was an outgoing guy. People liked him," Jones added. "But it's obvious by his actions he didn't care about anyone but himself."

International Corruption

U.S. Seeks to Recover \$1 Billion in Largest Kleptocracy Case to Date



FBI Deputy Director Andrew G. McCabe speaks at a press conference announcing U.S. efforts to recover more than \$1 billion in assets associated with a fund owned by the Malaysian government.

The U.S. government is seeking to recover more than \$1 billion in assets tied to international public corruption and a global money laundering conspiracy in what Department of Justice officials describe as the largest single action ever brought under the Kleptocracy Asset Recovery Initiative.

At a press conference today, Attorney General Loretta E. Lynch announced civil forfeiture complaints to recover assets associated with a fund owned by the Malaysian government that raised nearly \$8 billion to benefit the Malaysian people. Instead, much of the money was diverted by high-ranking fund officials and their associates to purchase yachts, hotels, a \$35 million jet, artwork by Vincent Van Gogh and Claude Monet, and to bankroll the popular 2013 film *The Wolf of Wall Street*.

"This fraud went on around the world," said Special Agent Darryl Wegner, chief of the FBI's International Corruption Unit,

which investigated the case along with the Internal Revenue Service's Criminal Investigative Division. "At least \$1 billion traceable to the conspiracy was laundered through the United States and used to purchase assets here."

From 2009 through 2015, according to the complaints, more than \$3.5 billion in funds belonging to 1Malaysia Development Berhad (1MDB) was allegedly misappropriated.

"When corrupt officials bring their ill-gotten gains to the United States, they also bring their corrupt practices and disregard for the rule of law."

The fund was created by the Malaysian government to promote economic development in that country through global partnerships and foreign direct investment. But members of the conspiracy—which included

1MDB officials, their relatives, and other associates—diverted billions of dollars using a web of shell companies with bank accounts in Singapore, Switzerland, Luxembourg, and the U.S. These complex schemes were intended to conceal the origin and ownership of the funds.

The FBI has three dedicated international corruption squads—in New York City, Los Angeles, and Washington, D.C.—to deal with foreign bribery incidents that are often tied to kleptocracy, the term used when foreign officials steal from their own governments at the expense of their citizens.

"That is basically what we saw in the 1MDB case," Wegner said. "And because these corrupt individuals used the U.S. banking system to hide or launder their criminal proceeds, the FBI took a lead role in investigating this matter." He noted that the criminal investigation is ongoing.



Attorney General Loretta E. Lynch discusses the 1MDB case. Other speakers included, from left, FBI Deputy Director Andrew McCabe; Leslie Caldwell, assistant attorney general for the Department of Justice Criminal Division; Eileen Decker, U.S. attorney for the Central District of California; and Richard Weber, Internal Revenue Service Criminal Investigation chief.

Investigators found that at least three sophisticated fraud schemes were used by those who misappropriated 1MDB assets. In 2009, through the use of shell companies, 1MDB officials and their associates allegedly embezzled approximately \$1 billion that was intended to be invested in an oil exploration joint venture with a foreign partner. Co-conspirators allegedly misappropriated another \$1.3 billion in funds raised through two bond offerings in 2012 and \$1.2 billion after another bond offering in 2013.

“Today’s action sends a message to corrupt foreign officials,” Wegner said. “The FBI, together with our international partners, will find these individuals and root out their corruption.” He added, “We are working very hard to make sure

that the U.S. will not be a safe haven for these types of crimes.”

“When corrupt officials bring their ill-gotten gains to the United States, they also bring their corrupt practices and disregard for the rule of law,” said FBI Deputy Director Andrew G. McCabe during today’s press conference in Washington, D.C. “That presents a threat to our economy, impacts trade and investment, fuels the growth of criminal enterprises, and undermines our fair democratic processes.”

The Malaysian people were defrauded “on an enormous scale,” McCabe said, adding that the fraud scheme “reached around the world,” making it “beyond any single agency’s ability to effectively investigate.” The FBI and the Department of Justice,

he explained, are “uniquely positioned” to investigate kleptocracy, and this case was a natural fit for the Bureau’s international corruption squads, which worked in conjunction with the Department of Justice, the Bureau’s overseas offices, and international partners including the Malaysian Anti-Corruption Commission.

Wegner noted that the leadership of the Malaysian Anti-Corruption Commission showed “tremendous courage” in pursuing the investigation, which was led by the FBI’s international public corruption squad in New York.

Fighting International Public Corruption

The Kleptocracy Asset Recovery Initiative was established in 2010 to curb high-level public corruption around the world. Led by a team of Department of Justice prosecutors working in tandem with the FBI and other federal law enforcement agencies, its mission is to forfeit the proceeds of corruption by foreign officials and, where appropriate, to use recovered assets to benefit the people who were harmed. Individuals with information about possible proceeds of foreign corruption located in or laundered through the United States should contact federal law enforcement or send an e-mail to kleptocracy@usdoj.gov.

Health Care Fraud

Three Charged in \$1 Billion Medicare Fraud Scheme



George Piro, special agent in charge of the FBI's Miami Field Office, is joined by (second from left) Wifredo A. Ferrer, U.S. attorney for the Southern District of Florida, and Department of Justice officials during a July 22, 2016 press conference announcing charges against three Miami-area health care providers in a case with losses in excess of \$1 billion.

Three Miami-area health care providers were charged today in a fraud scheme that resulted in more than \$1 billion in losses.

In what Department of Justice officials called the largest-ever criminal health care fraud case brought against individuals, prosecutors allege that Philip Esformes, 47, who owns more than 30 Miami-area skilled nursing and assisted living facilities (the Esformes Network), worked with a hospital administrator and a physician's assistant in an elaborate scheme lasting more than a decade to bill Medicare and Medicaid for procedures that weren't needed.

According to the indictment, Esformes and co-conspirators, Odette Barcha, 49, and Arnaldo Carmouze, 56, admitted unqualified beneficiaries to Esformes' network of nursing homes and assisted living facilities, where they then billed the federal health insurance programs for medically unnecessary services. The three are also alleged to have received kickbacks—often in cash or donations—for steering beneficiaries to other health care



Medicare Fraud Strike Force Locations. Image courtesy of HHS-OIG

providers, who also performed unnecessary treatments.

George Piro, special agent in charge of the FBI's Miami Field Office, described the losses as “staggering.” The FBI and the Department of Health and Human Services-Office of Inspector General investigated the case as part of the Medicare Fraud Strike Force.

“The investigators who unraveled this intricate scheme are to be commended for their diligence and commitment to root out fraud within our health care system,” Piro said Friday.

Since its establishment in 2007, the Medicare Fraud Strike Force has

Medicare Fraud Strike Force

Medicare Fraud Strike Force Teams harness data analytics and the combined resources of Federal, State, and local law enforcement entities to prevent and combat health care fraud, waste, and abuse. First established in March 2007, Strike Force teams currently operate in nine areas: Miami, Florida; Los Angeles, California; Detroit, Michigan; southern Texas; Brooklyn, New York; southern Louisiana; Tampa, Florida; Chicago, Illinois; and Dallas, Texas.

charged nearly 2,900 individuals who have collectively billed the Medicare program for more than \$10 billion.

Identifying the Vulnerabilities

Weapons of Mass Destruction Directorate Marks 10 Years



WMD training during a Nuclear Weapon Accident/Incident (NUWAIX) exercise in Seattle in 2015.



John Perren describes the WMD Directorate's National Improvised Explosives Familiarization (NIEF) course.

If you can imagine a disaster involving explosives or the release of nuclear, biological, chemical, or radioactive material, there's a pretty good chance a group of subject-matter experts within the FBI has built an elaborate scenario around it and tested how well emergency responders face up to it.

It's one of the main jobs of the Weapons of Mass Destruction (WMD) Directorate—to imagine worst-case scenarios and then devise ways to prevent and prepare for them. The Directorate was created 10 years ago this month, on July 26, 2006. John Perren, who has served as the WMD Directorate's assistant director since 2012 and was instrumental in its creation, said his team's job is to find gaps and vulnerabilities in the system and work to fix them.

"Countermeasures is the capital P-for-Prevention in the WMD Directorate," said Perren, who retires this month after nearly 30 years as an FBI agent. "That's where we sit down with academia, we sit down with the private sector, we sit down with the scientific community, and we describe to them what we view as the threat. Then together we decide: What are the gaps, what are the vulnerabilities, and how do we mitigate them?"

Given the nature of his job, Perren is often asked what his biggest worries are. "What keeps me up at night is not what I know. It's what I don't know," he has said in speeches, in testimony, and in briefings to members of Congress.

***"Together we decide:
What are the gaps,
what are the
vulnerabilities, and how
do we mitigate them?"***

The FBI has long had a role in preventing and investigating weapons of mass destruction. In 2005, FBI Director Robert S. Mueller recognized the need to elevate WMD matters with a focus on a more cohesive and coordinated approach. The WMD Directorate was officially established a year later. And Mueller tapped Dr. Vajid Majidi, the Department of Justice's chief science advisor, to serve as assistant director.

"The Directorate integrates and links all the necessary intelligence, scientific, and operational components to detect and disrupt the acquisition of WMD capabilities and technologies for use against the U.S. homeland by terrorists and other adversaries,"

Mueller said in testimony before Congress just six months after the WMD Directorate's formation.

The Directorate has three sections (see sidebar): countermeasures, investigations and operations, and intelligence. In its first five years, the Directorate established itself as a central hub for WMD subject-matter expertise. Over the past five years, Perren said, it has assumed a more operational posture, investigating hundreds of cases, providing scenario training for emergency responders, and establishing contacts and relationships in the communities where the FBI operates.

"We are intelligence driven," Perren said of today's WMD Directorate. "We have analysts embedded within different cells, but we also have tactical analysts with our operators in our investigations unit. We've done great things when it comes to investigations. We've been very proactive. We have undercover platforms. We have intelligence platforms. We work on the Dark Web. We work in all areas of the world."



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/wmdd10.

Defining Weapons of Mass Destruction

WMDs are defined as materials, weapons, or devices that are intended to cause or capable of causing death or serious bodily injury to a significant number of people through the release, dissemination, or impact of toxic or poisonous chemicals or precursors, a disease organism, or radiation or radioactivity, to include, but not limited to, biological devices, chemical devices, improvised nuclear devices, radiological dispersion devices, or radiological exposure devices.

The WMD Directorate

The Weapons of Mass Destruction Directorate (WMDD) exists to ensure the FBI and partners are prepared to anticipate, mitigate, disrupt, or respond to WMD threats. With the continued evolution of the WMD threat and the possibility of an overseas origin or nexus, the Directorate advances WMD prevention activities by supporting international WMD capacity building, developing plans and policies at strategic and operational levels, and developing partnerships, training, and outreach endeavors. By improving WMD security on a global level, the WMDD protects U.S. interests abroad and keeps WMD threats outside our borders. Today, the Directorate has three sections:

Countermeasures: The WMDD conducts prevention and outreach activities through FBI agents who

serve as WMD coordinators in each of the FBI's 56 field offices and in select overseas regional offices. Through these representatives, the Directorate heightens awareness of WMD threats, develops liaison relationships to mitigate these threats, and uses those relationships to identify evolving WMD threats. These liaison relationships are particularly critical in keeping the FBI abreast of new WMD threats and potential security vulnerabilities associated with technological advances. Tripwires are one example of a specialized, coordinated type of outreach where the FBI develops a network of experts—in law enforcement, public health, and industry, for instance—to assist if a threat emerges.

Investigations and Operations:

The WMDD investigates violations of WMD-related statutes and is responsible for coordinating, planning, training, and leading the FBI's response to the use or threatened use of WMD threats and incidents as a means of terrorism. The Investigations and Operations Section (IOS) within the WMDD is composed of six units that provide strategic management and oversight of the FBI's WMD program. The IOS is also responsible for operational response planning and coordination in support of field investigations and the mitigation of WMD threats and incidents. The IOS fields three regional WMD assistant legal attachés who address WMD and counterproliferation

situations by providing training at host government's request and ensuring a timely response for assistance to legal attachés and WMD events if pertinent.

Intelligence: The WMDD is staffed with a cadre of analysts who develop relevant, timely, actionable intelligence to identify, understand, and articulate WMD threats and vulnerabilities. The Directorate's intelligence analysts provide WMD subject-matter expertise and apply it to advise investigations and the U.S. Intelligence Community (USIC) regarding international and domestic terrorism, criminal/lone actors, critical infrastructure, and counterproliferation. WMDD analysts are involved in all aspects of the WMDD mission by providing strategic, domain, collection, and tactical analysis to WMD investigations and responses to WMD critical incidents. WMDD analysts collaborate with their counterparts in the FBI's Counterterrorism, Counterintelligence, and Laboratory Divisions. They serve on working groups providing subject-matter expertise with our intelligence community, other government agency, law enforcement, and private sector partners. Over the years WMDD analysts have provided briefings on various WMD topics to the FBI Director, Office of the Director National Intelligence, National Security Council, National Intelligence Council, U.S. congressional committees, our private sector partners, and many others.



Countering the Cyber Threat

New U.S. Cyber Security Policy Codifies Agency Roles

Earlier this year, the Obama Administration—in recognition of the growing cyber threat from criminals, terrorists, and others who wish to do us harm—released its Cybersecurity National Action Plan.

One aspect of this multi-layered plan was a specific focus on improving cyber incident response. Because the victim of cyber incidents is often a private sector entity, it's crucial that the private sector understands how the U.S. government will respond and coordinate in the event of a cyber incident impacting their networks, operations, or business.

So today, the Administration released Presidential Policy Directive-41 on U.S. Cyber Incident Coordination Policy, which sets forth principles that will govern the federal government's response to cyber incidents and designates certain federal agencies to take the lead in three different response areas—threat response, asset response, and intelligence support. Those agencies and their roles are as follows:

- The Department of Justice, acting through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), will be taking the lead on threat response activities;
- The Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, will be the lead agency for asset response activities;
- And the Office of the Director of National Intelligence, through its Cyber Threat Intelligence Integration Center, will be the lead agency for intelligence support and related activities.

As the lead for threat response, the FBI will play a key role in the event of a significant cyber incident, communicating with field-level coordinators on the ground to coordinate an effective, multi-agency response to the incident. Threat response activities include conducting appropriate law enforcement and national security investigative activity, like collecting evidence and gathering intelligence; mitigating the immediate threat; identifying disruption activities; and facilitating information sharing and operational coordination with asset response personnel.

“PPD-41 codifies the essential role that the FBI plays in cyber incident response, recognizing its unique expertise, resources, and capabilities.”

Additionally, according to the PPD, the FBI will also take part in the Cyber Unified Coordination Group, an entity to be formed in the event of a significant cyber incident that will also include asset response coordinators and, as appropriate, other federal agencies; local, state, and tribal governments; non-governmental organizations; the private sector; and international counterparts. This mechanism will take collaboration among all responding agencies to an even higher level.

The principles raised in PPD-41 that will guide the federal government's response to cyber incidents closely align with the FBI's values and priorities already in place when dealing with cyber incidents. The Bureau already

believes that:

- Prevention and management of cyber incidents is a shared responsibility among the government, private sector, and individuals;
- All incidents should be approached through a united federal government strategy that best uses the skills, authorities, and resources of each agency;
- The response will be based on an assessment of the risks posed to U.S. security, safety, and prosperity, and will focus on enabling the restoration and recovery of the affected entity; and
- The government will respect the privacy, civil liberties, and the business needs of victims of cyber incidents.

According to FBI Assistant Director James Trainor, Cyber Division, “PPD-41 codifies the essential role that the FBI plays in cyber incident response, recognizing its unique expertise, resources, and capabilities. And as the Bureau continues evolving to keep pace with the cyber threat, the authorities contained in PPD-41 will allow us to help shape the nation's strategy for addressing nationally-significant cyber incidents.”

“This new policy,” said Trainor, “will also enhance the continuing efforts of the FBI—in conjunction with its partners—to protect the American public, businesses, organizations, and the economy and security of our nation from the wide range of cyber actors who threaten us.”

'A Predator in Every Sense of the Word'

Subject Gets 70 Years for Theft Scheme and Producing Child Pornography

When a federal judge in Iowa sentenced 39-year-old Bradley Prucha to 70 years in prison last month, it was clear the intention was to ensure the registered sex offender with a long criminal history spend the rest of his life behind bars.

Among other charges, Prucha was convicted of being the ringleader of a multi-state retail theft scheme, producing child pornography, distributing a prescription narcotic to minors, and witness tampering.

"This man left a tremendous wake of victims and broken lives behind him," said Special Agent Kevin Kohler, who investigated the case from the FBI's Omaha Division. "He is a predator in every sense of the word."

In 2013, Prucha was released from a Florida prison for a retail theft scheme involving the use of counterfeit UPC bar code stickers. He placed bogus stickers on merchandise so items would ring up at a lower price. After purchasing the items, he then returned them for their full price or sold them online at a significant profit.

During his incarceration, his ex-wife relocated to Iowa, bringing their son with her. Prucha followed her there from Florida to fight for custody of the child, renting a room from a woman in Des Moines. Within a week, he had enlisted his new landlord in another bar code switching scheme.

"He saw that the woman was desperate for money," Kohler said, "and persuaded her they could both profit from his plan." Using specialized software obtained under false pretenses, Prucha printed counterfeit bar codes and, along with his accomplice, went



Bradley Prucha used counterfeit bar codes such as this one to cause retail merchandise to ring up below cost. Prucha—who also sexually exploited his teenage accomplices in the multi-state retail theft scheme—would then return the items for their full price or sell them online at a significant profit.

"shopping" in Illinois, Missouri, and Nebraska.

At his direction, the woman placed counterfeit bar codes over existing bar codes so that, for example, a \$400 electronics item would ring up for \$49. Prucha later recruited a 15-year-old girl he met through his ex-wife to participate in the scheme. Eventually, several of the teenager's female friends were also recruited.

Prucha was required to report monthly to his probation officer in Florida. He made the trip by car, taking the teens and hitting stores along the way. He provided the girls with the prescription drug Xanax and paid them to have sex with him. On several occasions, he filmed sexually explicit videos of himself with the minors. He also threatened them with violence when one girl learned about the videos—taken without her knowledge—and said she was going to call the police.

"For the most part, these were vulnerable teenage girls who didn't have stable home lives," Kohler said. "Prucha was able to recruit them by taking them on trips and buying them gifts and pretending to care about them when no one

else in their lives did."

In 2015, at a Barnes & Noble store in Chicago, Prucha's adult accomplice was arrested trying to make a fraudulent purchase. By that time, the theft ring had stolen so much merchandise from the chain that store security officers were on the lookout. The FBI was contacted, and the accomplice agreed to cooperate with authorities. She secretly recorded dozens of conversations in which Prucha detailed his criminal activity, including the sexual exploitation of the teenagers.

After his arrest in June 2015, while he was in jail awaiting trial, Prucha offered a fellow prisoner money to contact the girls he had abused and offer to pay them to change their statements. The inmate instead contacted the FBI. On March 1, 2016, a jury convicted Prucha on multiple charges; three months later, a judge imposed the 70-year sentence.

"To see the system work and see justice served in a case like this is very satisfying," Kohler said, adding that Prucha's lengthy sentence was justified. "There is no doubt in my mind that if he were released from prison, he would re-offend."

Victimized by a Cyber Scammer?

Don't Forget to File a Complaint with the IC3



As part of a campaign to increase awareness of the Internet Crime Complaint Center (IC3), digital billboards such as this are being displayed around the country.

Today, the FBI's Internet Crime Complaint Center (IC3) is embarking on a campaign to increase awareness of the IC3 as a reliable and convenient reporting mechanism to submit information on suspected Internet-facilitated criminal activity to the FBI. As part of the campaign, digital billboards featuring the IC3's contact information are being placed within the territories of a number of Bureau field offices around the country.

While the number of complaints being reported to the IC3 did increase in 2015 from the previous year, anecdotal evidence strongly suggests that there are many other instances of actual or suspected online frauds that are not being reported, perhaps because victims didn't know about the IC3, were embarrassed that they fell victim to a scammer, or thought filing a complaint wouldn't make a difference. But the bottom line is, the more complaints we receive, the more effective we can be in helping law enforcement gain a more accurate picture of the extent and nature of Internet-facilitated crimes—and in raising public awareness of these crimes.

The FBI field offices taking part in the billboard campaign include Albany, Buffalo, Kansas City, Knoxville, New Orleans, New York City, Phoenix, Oklahoma City, Salt Lake City, and San Diego. They were selected because they house multi-agency cyber task forces that participate in an IC3 initiative

called Operation Wellspring. This initiative connects state and local law enforcement with federal cyber resources and helps them build their own cyber investigative capabilities, which is important because not all Internet fraud schemes rise to the level necessary to prosecute them federally. We hope to expand Operation Wellspring to other FBI offices in the future.

Through the Wellspring initiative, IC3 personnel—using the complaint database and their analytical capabilities—create intelligence packages focused on particular geographic regions. These packages can highlight trends, identify individuals and criminal enterprises based on commonalities in complaints, link different methods of operations back to the same organization, and detect various layers of criminal activities. The packages also contain results of preliminary investigative research performed by IC3 analysts, including criminal records checks.

Once complete, these intelligence packages go to the appropriate FBI cyber task force and are then handed off to state and local task force members trained to investigate these kinds of crimes.

Beyond Operation Wellspring, the IC3:

- Forms alliances with industry representatives (online retailers, financial institutions, Internet service providers, etc.) that have increased the flow of the IC3's most valuable commodity—information.
- Makes its complaint database available to all sworn law enforcement (and FBI personnel) through the Bureau's secure Law

Enforcement Enterprise Portal. Accessing the database, users can get information on victims and financial losses within their particular area of jurisdiction to help build cases. Authorized users can also run a variety of statistical reports for themselves and can contact the IC3 for additional analytical assistance.

- Publishes an annual report highlighting the numbers and common types of complaints, along with emerging trends. The most recent *2015 Internet Crime Report* described the three major fraud types reported to the IC3 last year—business e-mail compromise, e-mail account compromise, and ransomware.
- Produces periodic public service announcements to alert consumers about the latest and/or emerging cyber crimes and provide tips on how to recognize them. Recent announcements covered tech support scams, stolen identity refund fraud, and the continuing threat from business e-mail compromise schemes.

Explains IC3 Unit Chief Donna Gregory, "IC3 is often the first piece of the investigative puzzle. We receive victim complaints and then analyze, aggregate, and exploit those complaints to provide law enforcement with comprehensive reports that can be used to open new investigations or enhance existing ones."

So if you or someone you know may have been victimized by a cyber fraudster, please submit a complaint to the IC3. And for additional information on filing a complaint, please review the IC3's Frequently Asked Questions page.

Health Care Fraud

Service Provider's Crimes Caused Patients' Deaths

A longtime Maryland health care provider was sentenced to 10 years in prison recently for cheating Medicare, Medicaid, and private insurers out of more than \$20 million—and causing patients to die as a result.

“This was an unusual case,” said Special Agent Keith Custer, who led the investigation from the FBI’s Baltimore Division. “Most health care fraud that results in injury or death happens when providers illegally bill for unnecessary procedures. This case wasn’t about providing unnecessary care, it was about denying people the care they desperately needed and deserved.”

Rafael Chikvashvili, a 69-year-old Baltimore resident, owned Alpha Diagnostics, a company that provided portable X-rays and other examinations to patients primarily in nursing homes and retirement communities in the Maryland area.

Beginning in 1997, Chikvashvili conspired with others to defraud Medicare, Medicaid, and other insurers in a variety of ways, including by creating false radiology reports that were never ordered or interpreted by a physician. What caused at least two patient deaths, according to court testimony, was that Chikvashvili instructed his non-physician employees—including Timothy Emeigh, the company’s vice president of operations, who was a radiologic technologist but not a doctor—to interpret X-rays instead of sending them to licensed physicians.

A non-physician Alpha Diagnostics employee reviewed one nursing home resident’s chest X-ray images and failed to detect congestive heart failure. As a result, the patient was not transferred to an acute care facility for treatment—

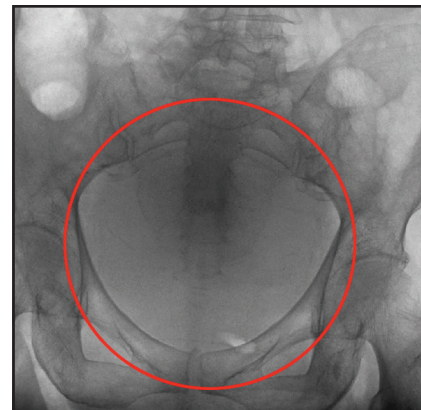
which is standard practice—but remained in the nursing home, where she died four days later. Had the patient been transferred, experts said, her symptoms could have been addressed.

A second patient had a chest X-ray as a pre-operative test to determine if she could safely undergo elective surgery. The non-physician Alpha Diagnostics employee who interpreted the X-rays failed to detect mild congestive heart failure. As a result, the patient was cleared for surgery, after which her congestive heart failure worsened. She died six days later.

“The vast majority of Alpha Diagnostic’s client base was from nursing homes and retirement communities,” Custer said. “This is an extremely vulnerable population,” he explained, “because it is not unexpected when they become sick and die. That was how Chikvashvili’s fraud was able to go on for nearly 20 years.”

In 2013, two Alpha Diagnostics X-ray technicians contacted authorities and said the company was upcoding—an illegal practice in which businesses bill insurance providers for more expensive services than were performed. The employees also said they suspected Emeigh was doing X-ray interpretations at Chikvashvili’s instruction and that real doctors’ names were being used fraudulently.

Custer and investigators from the U.S. Department of Health and Human Services Office of Inspector General began interviewing doctors whose names were on the X-ray reports. “It was clear from the beginning that the reports were fakes,” Custer noted. One of the doctors was living out



In this patient X-ray, the non-physician who interpreted the image failed to identify a large pelvic mass that was likely an infected bladder requiring immediate treatment. Because the ailment went undiagnosed, no treatment was provided, and the nursing home patient died the following day.

of the country when the reports with his name were created, and others confirmed that their names and provider numbers had been used fraudulently.

Chikvashvili, who holds a Ph.D. in mathematics but was never a medical doctor or licensed physician, claimed through his defense attorneys he was unaware of any wrongdoing and blamed the situation on actions by his employees. But a jury heard evidence to the contrary. In February 2016, he was convicted on a variety of charges related to the fraud and was sentenced in June. Emeigh, 52, had previously pleaded guilty to health care fraud and was sentenced to four years in prison.

Emeigh told investigators that prior to the fraud scheme being shut down, he was doing nearly 80 percent of Alpha Diagnostics’ X-ray interpretations in Maryland—readings that should have been done by a licensed physician. “He probably did tens of thousands of them over the course of the fraud,” Custer said. “There is no telling how many patients suffered or died because of these crimes.”

First Federal Spoofing Prosecution

Trader Sentenced in Case Involving Manipulation of Market Prices



It's often referred to as "spoofing"—but it's definitely no joke. Using computer algorithms or other means to manipulate commodity market prices in order to line your own pockets is a federal crime, a provision of the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act. And last month in a Chicago courtroom, a trader—after being convicted in the first-ever federal prosecution for spoofing under the 2010 law—was sentenced to federal prison.

Michael Coscia was the manager and owner of Panther Energy Trading, LLC, a high-frequency trading company based in New Jersey. He was also a long-time trader registered with the Commodity Futures Trading Commission (CFTC), a federal regulatory agency.

Evidence presented during his trial included testimony from his own computer programmer at Panther Energy Trading, who said that Cosca had designed two algorithm programs to be used for high-frequency trading and gave the programmer specific instructions on how he wanted the programs to operate. These programs worked as Coscia intended, moving the markets in a direction that was favorable to him. As a result, he was able to generate \$1.4 million in illegal profits between August and October 2011.

Coscia dealt in futures contracts, which are standardized, legally

binding agreements to buy or sell a specific product or financial instrument in the future. The buyer and seller of a futures contract agree on a price today for a product or financial instrument to be delivered or settled in cash on a future date. The type of trading that Coscia did—high-frequency trading—is a form of automated trading that uses computer algorithms to make decisions and place orders and is designed to enable traders to communicate with markets in milliseconds.

The contract markets Coscia worked in—like the Chicago Mercantile Exchange, the Chicago Board of Trade, and the New York Mercantile Exchange—are part of what's known as CME Group. And CME markets offer futures contracts in commodities like gold, soybean meal, soybean oil, and high-grade copper, as well as contracts that reflected changes in the value of the Euro and British pound against the U.S. dollar.

To place his trading orders, Coscia used servers physically located in Chicago that were part of a global electronic trading platform called Globex, operated by CME Group. His scheme—a variation of the "pump and dump" schemes that have been around since trading began—involved placing large-volume orders that he intended to cancel before they could be filled by other traders, thus creating a false impression about

the number of contracts available in the market. Other market participants would react to this deceptive market information and try to interact with the orders, pushing prices up or down, but the orders would disappear (yanked by Coscia's trading program). At the same time, Coscia was able to purchase contracts at prices lower than, or sell contracts at higher prices, than the prices available in the market before he entered his large-volume orders.

Coscia's scheme was eventually uncovered by the various exchange groups and regulators, and in July 2013, the CFTC ordered Coscia to return the \$1.4 million in illegal proceeds he had obtained and to pay an additional \$1.4 million civil penalty on top of that.

But it was about to get even worse for the trader. The FBI's Chicago Field Office, in conjunction with the U.S. Attorney's Office Securities and Commodities Fraud Section in Chicago and with the assistance of the futures exchanges, opened an investigation into his activities. After analyzing Coscia's trading records and interviewing his computer programmer, victims—which included representatives from other trading houses—and other individuals, Coscia was indicted by a federal grand jury in October 2014 on six counts of spoofing and six counts of commodities fraud. In November 2015, on the heels of a trial that lasted a little more than a week, Coscia was convicted on all 12 charges by a jury that came to its decision in about an hour.

Another reminder that the FBI places a high priority on investigating crimes that threaten the fairness of our markets and the confidence of investors.

Murder for Hire

Alaska Man Wanted Federal Agents Killed

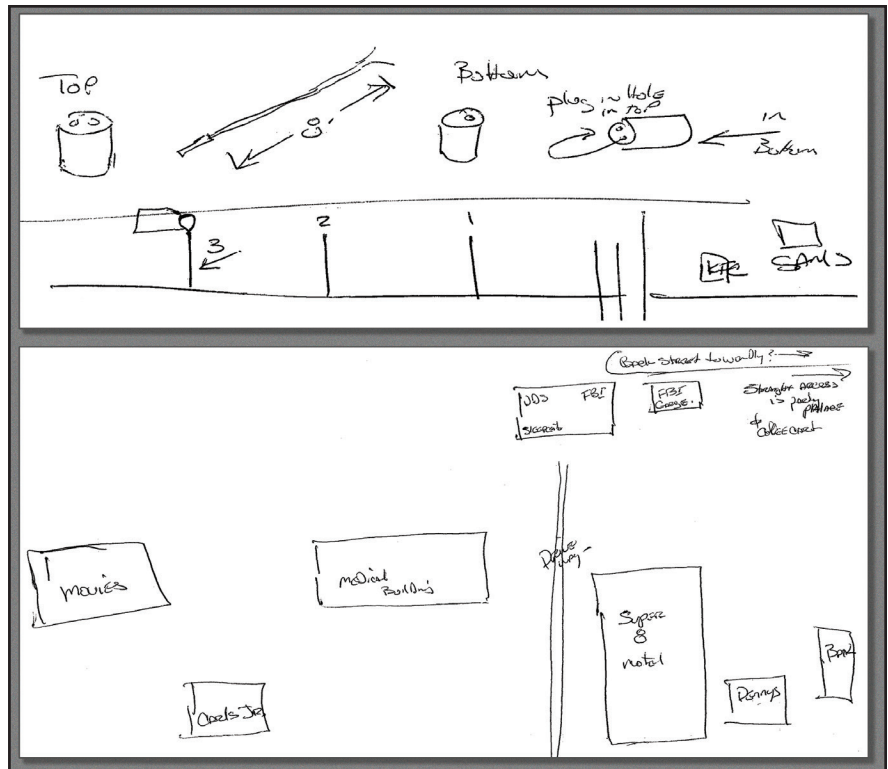
Chris Guy Mannino, a former chiropractor and gun and explosives dealer who lived in Fairbanks, Alaska, had scores to settle—and murder was how he planned to settle them.

After a messy divorce that did not go his way—in part because he had filed for bankruptcy and was under felony indictment for weapons charges—Mannino hired a hit man to kill his wife's attorney. When the would-be killer turned out to be cooperating with the FBI, Mannino later hired a second individual to kill the original hit man. And his murderous intentions didn't stop there.

"He had a hit list," said Special Agent Derik Stone, one of the investigators who worked the case from the FBI's Anchorage Division. That list included federal law enforcement personnel, including an FBI agent and two agents from the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF).

"He wanted to kill the FBI agent, the main witness in the weapons case, and the individual he initially hired as a hit man," Stone said. "He also wanted to kill a bankruptcy attorney and both ATF agents who investigated his case."

Instead, the 57-year-old Mannino is in prison, having been recently sentenced to a 17-year term on a number of charges related to the murder-for-hire plot. Mannino's problems began with financial issues. "He got in over his head and decided to file for bankruptcy," Stone said. "But he tried to hide assets, including guns, in his wife's name. And he also transferred an unregistered machine gun to another person without proper paperwork, which is a felony."



A sketch instructs a would-be hit man how to build a bomb. Another diagram points to the FBI's Fairbanks office.

The one-time president of the Alaska Machine Gun Association was indicted by a federal grand jury in August 2013 for a number of charges related to the unlawful possession and transfer of prohibited weapons, including a machine gun and silencers. In 2014, while awaiting trial on those charges and others related to his bankruptcy, Mannino hired a hit man to murder the attorney.

After the plan unraveled and he was in custody at the Fairbanks Correctional Center, Mannino attempted to hire another hit man—a fellow prisoner about to be released to a halfway house—to kill the original hit man and carry out the other murders. He told that individual where to find a cache of explosives, instructed him on how to shape explosive charges for maximum effect, and drew a map of the FBI office in Fairbanks. He made specific and gruesome

requests. He wanted the hit man to travel to Tennessee, for example, to kill one of the ATF agents and then rig the graveside with a bomb so it would kill everyone else who came to the funeral.

Fortunately, the second would-be hit man contacted authorities. Mannino was federally indicted again in 2015, this time for soliciting murder. After a four-day trial in February 2016, he was found guilty. Imposing his sentence in June, a federal judge in Fairbanks noted the jury's conclusion that Mannino intended for the murders to actually occur, rather than his conduct simply being "jail house talk" between inmates as Mannino had contended.

"He was angry, and he was serious about the killings," Stone said. "He had the tools and capabilities to do what he said he was going to do."

Cadre of Special Agent Candidates Gathers in D.C.

Recruiting Event Supports FBI Commitment to a Diverse Workforce



Candidates line up at a recruiting event in Washington, D.C. for qualified special agent candidates of diverse racial and ethnic backgrounds.

“I want to ensure diversity is a part of the DNA of the FBI...until it becomes who we are.”

So said FBI Director James B. Comey earlier this week at a Bureau-sponsored gathering in Washington, D.C. for qualified special agent candidates of varied racial and ethnic backgrounds. During the Diversity Agent Recruitment event for aspiring agents, Comey told participants that diversity is a priority within the Bureau because a diverse workforce is a strong workforce.

The August 17 information session was designed for highly

qualified, diverse applicants from the Washington, D.C. metro area, but drew hundreds of applicants from around the country as well. Participants learned firsthand about the skills and competencies required to become agents. They also had the opportunity to speak with current FBI agents who shared their own on-the-job experiences.

In addition to Comey and other FBI personnel, the event featured a keynote speech from retired former FBI Executive Director Mike Mason, who encouraged applicants to see past any possible mistrust or misgivings about joining law

enforcement and follow their passion to serve. “Never give up,” Mason said. “Be the person you know you are.”

This week’s event was one component of the FBI’s overall commitment to building and maintaining a diverse and inclusive workforce in order to connect with the communities we serve. More informational sessions and outreach events are planned for cities and college campuses throughout the country.

Artifact of the Month

Historical Items Featured on FBI Social Media Accounts

The FBI's Artifact of the Month project highlights FBI artifacts and cases to give insight into our mission and our work around the country and the world. Below are some of the artifacts featured on our social media accounts (Twitter, Flickr, and Facebook) in 2016. #ArtifactoftheMonth



April: Unabomber Bomb Shrapnel

April 3, 2016 was the 20th anniversary of the arrest of Theodore "Ted" Kaczynski, widely known as the Unabomber. Shown is shrapnel from a 1987 bombing of a computer store in Salt Lake City carried out by Kaczynski.



July: D.B. Cooper Plane Ticket

A man calling himself Dan Cooper paid cash for this plane ticket on November 24, 1971. He hijacked the plane and later parachuted out with ransom money, never to be seen again.



May: Robert Hanssen

Shown are convicted spy Robert Hanssen's FBI business cards as well as pieces of white chalk and thumbtacks he used to leave messages for his Russian handlers.



August: Olympic Torches

The Olympic Torches from both the 1988 Summer Olympics in Seoul and the 2002 Winter Olympics in Salt Lake City were given to the FBI in appreciation for the Bureau's ongoing support in ensuring the safety of the events.



June: "Baby Face" Nelson's Body Armor

"Baby Face" Nelson's body armor was recovered on November 27, 1934 after the shootout in Barrington, Illinois that resulted in the death of FBI Special Agent Herman Edward Hollis and ended Nelson's life.



September: Ground Zero Flag

This American flag is from Ground Zero in New York City. On the 15th anniversary of 9/11, we remember those who lost their lives in the attacks. We also honor the memories of those who gave their lives to save others, including FBI Special Agent Lenny Hatton and former FBI Special Agent in Charge John P. O'Neill.



Scan this QR code with your smartphone to see all Artifacts of the Month on the FBI's Flickr page, or visit www.flickr.com/photos/fbi/albums.

FBI Releases New Bank Robbers Mobile App

Asking for Help in Identifying Unknown Suspects



Back in December 2012, the FBI launched its Bank Robbers website featuring a gallery of unknown bank robbery suspects wanted by the Bureau. Because the FBI, in its own bank robbery investigations, focuses on the most violent and/or the most prolific serial offenders who often cross jurisdictions, the suspects included on bankrobbers.fbi.gov are a dangerous lot and public assistance in identifying them plays a crucial role in our efforts to apprehend them.

Today, we're enhancing our efforts to publicize these dangerous criminals by launching our mobile Bank Robbers application for iPhones (plus iPads and iPods) and Android smartphones, which should make it even easier for the public—as well as financial

institutions, law enforcement agencies, and others—to view photos and information about bank robberies in different geographic areas of the country. The app, which works with bankrobbers.fbi.gov, can be downloaded for free from Apple's app store or Google Play.

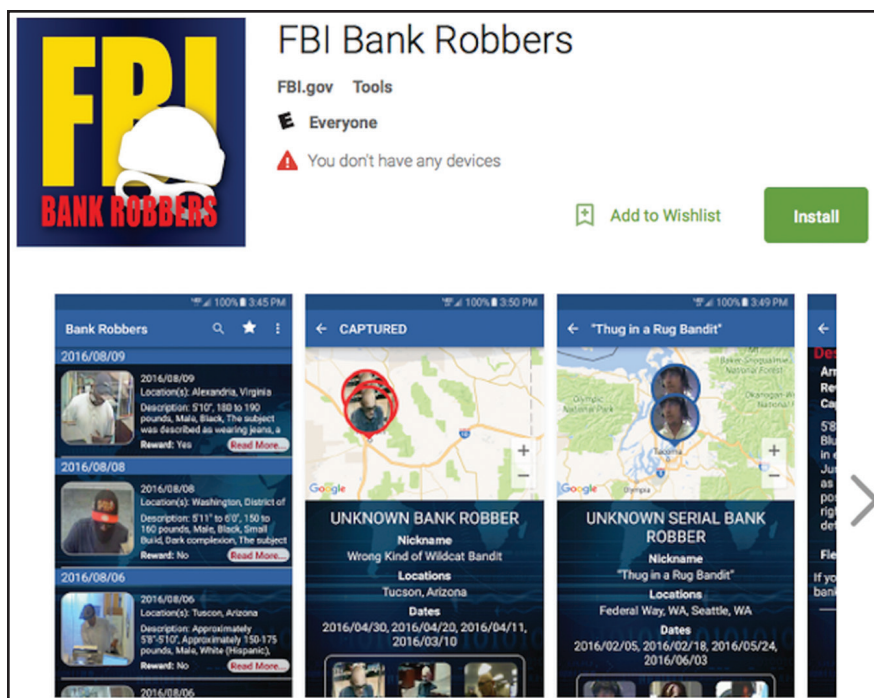
Using the app, bank robberies can be sorted by the date they occurred, the category they fall under (i.e., armed serial bank robber), the FBI field office working the case, or the state where the robbery occurred. If the location services on your device are enabled, you can view a map that shows the relevant bank robberies that took place in your geographic area. You also access surveillance photos, physical description information, robbery details, and the FBI's

wanted poster for each suspect. Users can select push notifications to be informed when a bank robbery has taken place near their location.

Additionally, the app provides quick access to a link directly to the FBI online tips page so users can contact us immediately if they have information on any of the robberies or suspects.

Some of the unknown bank robbers currently being sought by the FBI include:

- A suspect, wanted for nine bank robberies in Maryland, Virginia, and West Virginia, who displayed, at various times, handguns and even a sawed-off shotgun during eight of those robberies.
- Another suspect, wanted in



The Bank Robbers mobile app is available for download on iPhone and Android devices.

connection with 11 bank robberies in Pennsylvania, who either carried or wore a semi-automatic handgun while verbally demanding money.

- In California, a suspect who reportedly wears various disguises and has committed four bank robberies while displaying a handgun.
- And in Phoenix, a suspect who entered a bank, pushed an elderly woman out of his way, and pointed a handgun at bank employees and customers demanding money.

According to the FBI's bank crime statistics for 2015, there were 4,091 robberies, burglaries, and larcenies committed under the federal bank robbery statute in a variety of financial institutions—including commercial banks, savings and loan associations, credit unions, and armored carrier companies. Demand notes were a favorite tool used by bank robbers (2,416 times), but actual firearms were used 877

times, the threat of weapons was used 1,762 times, and explosive devices used or threatened occurred 108 times.

"We focus our investigative resources on those suspects who pose the greatest safety threats to the public, and our new Bank Robbers mobile app is another tool we can use to help mitigate those threats."

That's certainly proof that these crimes—and these criminals—can be extremely dangerous. And during 2015, actual acts of violence—from discharging a firearm to setting off explosives to committing assaults—were committed in 137 of the 4,091 incidents. Unfortunately, these violent acts led to 57 injuries, nine deaths, and 66 people being taken hostage.

Bank Robbers Website Success Story

The FBI's Bank Robbers website—and the new Bank Robbers mobile app—were created to help publicize unknown violent and/or serial bank robbery suspects who are wanted by the Bureau. The publicity works and really does help to get dangerous criminals off the streets.

Here's a bankrobbers.fbi.gov example:

After the website featured a suspect believed to have been responsible for 11 armed takeover style robberies in Delaware and Pennsylvania, local police received a tip in the mail which broke the case open—a printed page from the Bank Robbers website featuring the unknown suspect believed responsible for the robberies. Across the piece of paper was a handwritten name. A subsequent investigation led to the positive identification of the suspect as well as charges being filed against him in both states. That suspect is currently awaiting trial.

The FBI has always depended on the assistance and the support of the public in carrying out its mission, beginning back in its early days when some of our wanted criminal posters were tacked up onto post office walls. But today's technology—like websites and apps—can work as force multipliers and allow us to ask for and receive assistance from larger segments of the public.

The FBI continues to provide assistance to state and local partners investigating bank robberies, according to Gregory Adams, chief of the FBI's Violent Crimes Unit in Washington, D.C. "But we focus our investigative resources on those suspects who pose the greatest safety threats to the public" he explained, "and our new Bank Robbers mobile app is another tool we can use to help mitigate those threats."

Fugitive Apprehended

Alleged Child Abuser Was on the Run for 23 Years



In 1993, Boston-area resident John Hartin was 23 years old when he befriended two young boys—ages 6 and 9—and allegedly raped them.

One of the victims eventually told a family member about the abuse, which led to an investigation and Hartin being charged in Massachusetts with five counts of rape of a child. Rather than face the charges, Hartin fled, and was later charged federally with unlawful flight to avoid prosecution.

He was at large for more than two decades, and investigators followed numerous leads without success. “But the case never stopped being actively investigated,” said Special Agent Brooks Broadus, a member of the FBI’s Boston Division Child Exploitation Task Force. “We were always looking.”

At the time of his disappearance, Hartin, a lifelong resident of Dorchester, Massachusetts, was working as a security guard. He had also studied graphics and computer arts in college. His first alleged victim was related to an acquaintance of Hartin’s. The young boy’s close friend was Hartin’s second alleged victim.

In 2012, the FBI launched a multi-state media campaign and announced a reward of up to \$25,000 for information leading to Hartin’s arrest. The campaign generated thousands of tips—and many tantalizing leads—but no arrest.

“It was old-fashioned detective work that led to Hartin’s capture.”

More recently, explained Boston Police Department Det. Mike Sullivan, a member of the Child Exploitation Task Force, “we started looking at the case again with fresh eyes and went back to day one. We sought out Hartin’s family and friends and began to conduct new interviews.”

In the end, Sullivan said, “it was old-fashioned detective work that led to Hartin’s capture.” Sullivan reached out to various law enforcement agencies, including the U.S. Marshals Service and the U.S. Department of State, for assistance in the search. Through these partnerships, investigators learned that Hartin was using the alias Jay Carter. The fugitive had

a driver’s license in Carter’s name and other fraudulent documents.

Leads were initially sent to the FBI Miami Division, FBI Long Beach Resident Agency, and the FBI Greensboro Resident Agency. The fugitive was traced to Walkertown, North Carolina, and the FBI put his residence under surveillance. Intelligence revealed that he had weapons in the house. “We had information that he was armed and potentially dangerous,” Sullivan said. Although Hartin was taken into custody without incident at his home on June 15, 2016, he initially denied his true identity.

“We are still piecing together where he was for all the years he was on the run,” Broadus said. “He lived in Florida for a long period of time before he went to North Carolina. We also had information he may have lived in California. He apparently did freelance computer work to earn money and worked in a bar in Miami.” Broadus added that Hartin had roommates and “significant others who might have helped him financially. They all deny they knew his real identity.”

Hartin, now 46 years old, was on the run for 23 years. He waived extradition, and U.S. Marshals recently returned him to Massachusetts, where he will now have to answer for his actions in court.

Broadus commended the Boston Police Department and federal law enforcement partners for their efforts on the case. After Hartin’s arrest, Sullivan and Suffolk County Assistant District Attorney Alissa Goldhaber contacted the victims to let them know Hartin had finally been captured. After learning the news, one victim said, “This is the best day of my life.”

Take the Safe Online Surfing Internet Challenge

Available Soon for 2016-2017 School Year



What do more than 870,000 students across the nation have in common?

Since 2012, they have all completed the FBI's Safe Online Surfing (SOS) Internet Challenge. Available through a free website at <https://sos.fbi.gov>, this initiative promotes cyber citizenship by teaching students in third through eighth grades how to recognize and respond to online dangers through a series of fun, interactive activities.

Anyone can visit the website and learn all about cyber safety, but teachers must sign up their school to enable their students to take the exam and participate in the national competition. Once enrolled, teachers are given access to a secure webpage to enroll their students (anonymously, by numeric test keys) and request their test scores. E-mail customer support is also provided. Top-scoring schools

each month are recognized by their local FBI field office when possible. All public, private, and home schools with at least five students are welcome to participate.

Now entering its fifth season, the FBI-SOS program has seen increased participation each year. From September 2015 through May 2016, nearly a half-million students nationwide finished the activities

and took the exam. We look forward to even more young people completing the program in the school year ahead. The challenge begins September 1.



Scan this QR code with your smartphone to access <https://sos.fbi.gov>.

A Sampling of Teacher Comments from the 2015-2106 School Year

"My 3rd, 4th, and 5th grade students LOVE Cyber Surf Islands!"

"We will begin using your site! It's awesome!"

"We have been in your program for the last three years and have gotten good response from the students and parents about your program."

"Thank you for providing a wonderful learning experience for students."

"I love the program and want my students to participate."

"This was a very good exercise. I plan on doing it again next year."

"Thank you for such a great resource!"

1991 Talladega Prison Riot

A Look Back at the FBI's Early Crisis Response Capabilities



Twenty-five years ago this month, the FBI—working closely with our partners at the Federal Bureau of Prisons (BOP)—played a crucial role in the successful resolution of a prison riot that ended without loss of life or serious injury to any of the hostages, inmates, or responding federal officers.

From August 21 through August 30, 1991, at the Federal Correctional Institution (FCI) in Talladega, Alabama, approximately 120 Cuban detainees armed with homemade weapons took seven BOP and three Immigration and Naturalization Service (INS) employees hostage. The Talladega detainees—a small portion of the more than 120,000 Cubans who came to the U.S. during a six-month period in 1980 in what was called the Mariel boatlift—were being held on a variety of criminal charges. The men had exhausted their appeals through the U.S. legal system and were to

be sent back to Cuba, but they didn't want to go.

The incident began in FCI Talladega's Alpha Unit—the maximum security wing—around 10 a.m. on August 21, 1991. Negotiations began, and inmates demanded—among other things—that they not be returned to Cuba. Within a few hours of the takeover, Acting U.S. Attorney General William Barr tasked the FBI with the tactical response to the hostage situation: If negotiations failed, the Bureau was to take the lead.

The FBI's Birmingham Field Office responded first, with Special Agent in Charge Allen Whitaker and his crisis response team quickly mobilizing and setting up a command post. The FBI's Hostage Rescue Team (HRT) and Special Weapons and Tactics (SWAT) teams from Birmingham and Atlanta were mobilized as well. There was soon a presence of about 180 FBI agents and

specialized personnel joining BOP's Special Operations Response Teams (SORT) and additional personnel from the BOP, the U.S. Marshals Service, and INS. At FBI Headquarters, our Strategic Information Operations Center was also stood up to monitor the situation.

It was hoped that the situation could be ended quickly. In earlier prison riots by Cuban detainees at federal facilities in Atlanta, Georgia and Oakdale, Louisiana, federal negotiators had been able to resolve each crisis. But this time seemed different.

Talks at FBI Talladega—conducted by both BOP and FBI negotiators—were intermittent through the first several days and slowed even further as the incident stretched into its sixth and seventh days. Inmates began firing homemade arrows out of the prison wing and appeared to be fortifying the roof. Some displayed



Left: The federal prison in Talladega, Alabama was the site of a 1991 riot in which detainees held 10 federal employees hostage for more than a week. (Bureau of Prisons photo)

messages written on bed sheets to communicate directly with members of the media outside the prison.

On the eighth day, one hostage was released for medical care, but the approach of the prisoners was hardening and the situation was deteriorating. And the next day, inmates announced they would begin killing hostages one by one,

drawing names from a pillow case, if certain interim demands were not met.

All Department of Justice representatives, including Acting Attorney General Barr and the BOP and FBI directors, considered this threat real and of immediate concern. And late on the evening of August 29, Barr gave the order to free the hostages.

So at 3:40 a.m. on August 30, 1991, the Bureau's HRT and SWAT teams joined the BOP's team and entered the building. Using shaped charges, they blew off the fortified door to a room holding the hostages and rescued them all without injury. And SORT members took control of the prisoners.

To better facilitate the Bureau's rapid response to critical incidents, the FBI in 1994 formally created the Critical Incident Response Group (CIRG) to integrate tactical, negotiation, behavioral analysis, and crisis management resources into one cohesive structure.

Since then, the FBI's mission has expanded and evolved, as have CIRG's responsibilities, which today also include hazardous device disruption, surveillance, special events management, and training for Bureau field personnel and domestic and international law enforcement partners.

And CIRG experts remain on call 24 hours a day, seven days a week, to respond in the event of a crisis.

Personal Reflections from Talladega

Excerpted from "The Hostage Rescue Team, Part 5: Held to a Higher Standard" on www.fbi.gov

Retired Special Agent Jaime Atherton helped pioneer the HRT's use of explosive breaching to gain entrance into fortified places during crisis situations. In 1991, he was part of the team that helped rescue nine hostages held by Cuban inmates in the Talladega federal prison in Alabama. The Cubans had been incarcerated after the Mariel boatlift in 1980 and were rioting to prevent their return to Cuba.

"We were there eight or nine days during the standoff and negotiations when the Cubans threatened to kill some of the hostages," Atherton recalled. "And because they had nothing to lose, they were taken very seriously." The acting attorney general gave the FBI the green light to rescue the prisoners, and the HRT led the way.

The Cubans and their hostages were barricaded behind bars in a section of the prison, and as Atherton pointed out, it's much easier to break out of a prison than into one. But when his team got the word, operators executed the type of explosive breach they had trained for—and it worked flawlessly. The hostages were rescued unharmed, and none of the Cubans were hurt.

"That was our first significant use of explosive breaching," Atherton said, "and to do it in a maximum security prison with people's lives at stake—that was a pretty big moment for us, a pretty intense couple of minutes. That's where all your training pays off."

Chicago Cold Case

Seeking Justice for a Murdered Teenage Girl



Murder victim Alexandra (Alex) Anaya was reported missing from her home in Hammond, Indiana on August 13, 2005.

Thirteen-year-old Alexandra Anaya was brutally murdered 11 years ago this month, and today the FBI's Chicago Division—in close partnership with local authorities—marked the anniversary by requesting the public's assistance to help to solve the case.

The Indiana teen, known to friends and family as Alex, was reported missing from her home August 13, 2005—she was last seen by her mother early that morning. Three days later, boaters on the Little Calumet River in Chicago found her dismembered body floating in the water.

Both the Chicago Police Department (CPD) and the Hammond Police Department in Indiana conducted an exhaustive investigation at the time and have continued to follow leads since, but Alex's killer remains at large. Her case is one of many now being reviewed by FBI Chicago's recently established Homicide Initiative Task Force.

"We believe this was not a random

act of violence and that Alex knew her assailant," said FBI Chicago Special Agent in Charge Michael J. Anderson during a press conference today in Chicago. "It has been more than a decade since Alex was murdered, and during that time people and relationships have changed. We are hopeful that someone will come forward now," he added.

The Homicide Initiative Task Force—a collaboration between the FBI and the CPD—was launched in April 2016 to help local authorities solve some of Chicago's most violent murders. Task force members re-examine cold cases with a fresh perspective and take advantage of the most current scientific techniques and forensic processes.

"The homicide rate is extremely high in Chicago," said Special Agent Courtney Corbett, a task force member who works alongside CPD detectives and other FBI personnel. "Because there are so many homicides here, a cold case could be 20 years old or a murder

that occurred six months ago."

CPD homicide detectives often have caseloads that are overwhelming, Corbett said. "The task force is here to provide specialized assistance and help in any way we can." That assistance translates into FBI resources such as enhanced DNA testing, telephone record analysis, surveillance, and the deployment of Bureau experts, including dive team personnel and members of the Behavioral Analysis Unit—commonly called profilers.

In Alex's case, Corbett said, "we have been reviewing leads and re-interviewing individuals associated with this case. The DNA evidence has been well preserved, and we plan to use enhanced technology to exploit that evidence." She added that task force members are fully invested in finding the killer. "We want to bring justice to Alex and other victims like her, and their families," Corbett said. "To do that—and to ultimately reduce the homicide rate in Chicago—we all have to work together."

Anyone with information regarding the murder of Alex Anaya—no matter how insignificant they think it might be—is asked to contact the FBI's Chicago Field Office at (312) 421-6700 or submit a tip online.

Note: This case may have been resolved since this information was posted on our website. Please check www.fbi.gov/wanted for up-to-date information.

Future Agents in Training

High School Students Get Inside Look at FBI Careers



It was just before noon when explosives detonated inside four cars on a grassy field near the FBI Training Academy in Quantico, Virginia. Shortly after the blasts, a group of high school students loaded up equipment and made their way downrange to investigate.

It was a textbook post-blast crime scene for the Bureau's Evidence Response Teams, only this scenario was part of a weeklong course for teenagers interested in career opportunities with the FBI.

Since 2008, the FBI's Washington Field Office (WFO) has hosted the annual Future Agents in Training (FAIT) program, which provides a hands-on approach to educating area high school juniors and seniors on the Bureau's operations. With a focus on becoming a special agent, the program presents a cross section of the FBI, including its criminal, counterterrorism, intelligence, and administrative divisions.

"The high school students who attend the FAIT program are among the best and the brightest from our region," said WFO Assistant Director in Charge

Paul Abbate. "While youth today are exposed to stories about law enforcement in the news and on dramatic television shows, the program provides a realistic, behind-the-scenes look into life in the FBI."

This year, a stop at the Explosives Unit range was included in the week's curriculum. Students learned how the unit investigates bombings and responds to suspicious packages. Various stations were set up to display equipment and technology, while live demonstrations were provided to simulate ordnance explosions at varying degrees of intensity.

The highlight of the day included the post-blast investigation, where the students learned how to collect evidence following an explosion and determine the type of device used in the detonation.

"It was like being in a TV show where a crime is solved in one hour," said Raven, a FAIT program participant. "That's literally what we got to do. It was fun acting as an investigator or crime scene analyst for a day."

For Benjamin, another participant, simply experiencing the day-to-day operations of the FBI has influenced his career decisions. Having completed the course, he said he's considering applying to become either a special agent or intelligence analyst after obtaining a law degree.

"Having the ability to come and see what it's like to be a member of the FBI and seeing the diverse roles really impacted me when it comes to choosing my career," Benjamin said.

The post-blast investigation exercise served as a culminating experience for the students. While next year's curriculum may integrate different training areas and practical exercises, the result remains the same: prepare students for a future career in the FBI.

"After attending this program, students walk away with a real-life understanding of the commitment and character needed to be an FBI employee. I have no doubt that we will see many of these promising young adults return to the FBI as agents, analysts, and professional staff," said Abbate.

Remembering 9/11

FBI Has Evolved in Response to Changing Threats



A U.S. flag adorns the landscape at the National 9/11 Pentagon Memorial in Arlington, Virginia.

This weekend, the FBI joins the nation in remembering and honoring the victims of the 9/11 terror attacks, which occurred 15 years ago this month.

It was then that the Bureau began the most massive investigation in its history, after terrorists hijacked and crashed four commercial airliners—two at the World Trade Center in New York, one at the Pentagon, and one in a field in Shanksville, Pennsylvania—killing 33 crew members, 213 passengers, and 2,730 people on the ground. Thousands more were injured.

Since the attacks of 9/11, the FBI has transformed from a reactive, investigative-led model to a proactive, intelligence-driven one where intelligence informs our investigative strategies, enhances our understanding of terrorism threats, and increases our ability to address and mitigate these threats. The terrorism threats against the U.S. have evolved since 2001, but they remain, according to

Director James Comey, “persistent and acute,” especially those posed by individuals who are recruited domestically and travel abroad to join the Islamic State of Iraq and the Levant (ISIL), and by homegrown violent extremists who may aspire to attack the United States from within.

“The FBI continues to strive to work and share information more efficiently and to pursue technological and other methods to help stay ahead of threats to the homeland.”

In response to these evolving threats, the FBI uses all lawful investigative techniques and methods at its disposal. With our domestic and foreign partners, the Bureau collects and analyzes intelligence information as it pertains to foreign terrorist

organizations and homegrown violent extremists. We also encourage information sharing, working closely with the many federal, state, local, and tribal agencies assigned to our Joint Terrorism Task Forces around the country.

“Rest assured,” said Comey, speaking before a congressional committee earlier this year, “the FBI continues to strive to work and share information more efficiently and to pursue technological and other methods to help stay ahead of threats to the homeland.”

The Bureau also strives, on a daily basis, to ensure the safety of the American public from the threat of terrorism and other crimes while safeguarding citizens’ constitutional rights.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/15years911.

Human Trafficking

Guatemalan Migrants Exploited in Forced Labor Scheme

Aroldo Castillo-Serrano made big promises to parents in his Guatemalan community—that a good education and a better way of life awaited their children in the United States. Instead, the minors and adults he lured to Ohio were forced to work on egg farms and live in deplorable conditions.

The Guatemalan parents agreed to pay Castillo-Serrano upwards of \$15,000 to take their children to the United States, where they would go to school and have good-paying jobs to help pay back the debt. Since the parents could not afford the fee up front, they gave Castillo-Serrano the deeds to their properties as collateral.

With the help of co-conspirators, Castillo-Serrano smuggled the victims across the border, forced them to live in an isolated trailer park, and used threats of physical harm to compel them to work on the egg farms.

“We think the scheme was going on as early as 2011,” said Special Agent Matthew Komar, an investigator on the case from the FBI’s Cleveland Division. “The youngest trafficking victim we found was 14 years old.”

In late 2014, a tip to a human trafficking hotline made its way to the FBI through the United States Attorney’s Office for the Northern District of Ohio, and an investigation was begun. Surveillance was conducted at the trailer park, and probable cause search warrants were obtained for 16 dwellings.

When the search warrants were executed in December 2014—in conjunction with local authorities and U.S. Immigration and Customs Enforcement-Homeland Security Investigations—nearly 60



people were temporarily removed. “The trailers were in pretty bad condition,” Komar said. “Some had running water, some did not. Some didn’t have heat. Some didn’t have bathrooms. Some had holes in the floors. Dilapidated is a generous term to describe them.”

When they were smuggled across the border, Komar said, “some of the young victims were promised they would be going to school—that never happened. They were put to work right away.”

The victims were picked up by a crew chief in the morning and taken to the farms to work physically demanding 12-hour shifts that included cleaning chicken coops, loading and unloading crates of chickens, and removing the beaks from chickens.

“When they were paid,” Komar said, “victims gave their checks to Castillo-Serrano or his associates, and they got back approximately \$50. When some of the juveniles complained, they were threatened physically, and their families in Guatemala were threatened if they didn’t work.”

Eventually, investigators identified 10 victims—eight minors and two adults—whose statements would

make the case against Castillo-Serrano. A co-conspirator in the scheme, Ana Angelica Pedro-Juan, falsely represented herself to government officials as a family friend of the minor victims so they would be released to her if the juveniles were caught at the border. She also oversaw the trailers where the victims were housed.

In 2015, Castillo-Serrano pleaded guilty to charges of forced labor and alien harboring. Pedro-Juan pleaded guilty to conspiracy to commit forced labor. In June, Castillo-Serrano, 33, was sentenced to more than 15 years in prison, and Pedro-Juan, 22, received a 10-year term. They were also ordered to pay more than \$67,000 in restitution to the victims. Most of the property deeds have been returned to the families of the victims, and four other co-defendants have also received jail terms.

“This case is ongoing,” Komar said. “We believe there are still people who were complicit in the scheme. He added, “When people think of human trafficking, they usually think of sex trafficking. But forced labor is real, and it is eye opening when you see the damage it can do.”

Report from Thailand

Part 1: Confronting the Child Sex Trade in Southeast Asia



Thailand has long been a popular tourist destination for Westerners charmed by the country's culture and cuisine, its storied beaches, and its ever-present markets. Unfortunately, a certain type of visitor is also drawn to the well-established sex trade, which too often victimizes children.

The dark side of Thailand's tourism industry plays out nightly in Bangkok's tawdry red-light districts, in Chiang Mai's after-hours club scene, and along the neon-infested Walking Street in the coastal town of Pattaya. In these and other places less obvious, trafficked children can be bought and sold, reduced to the basest form of commerce.

Increasingly, the Thai government—with the assistance of the FBI and other partners—has taken significant steps to address the sexual exploitation of children and to focus more attention on victims, whose interests in the past have sometimes been overlooked.

"The Thai government has adopted a new urgency when it comes to the issues of child exploitation, sexual abuse, and trafficking in persons," noted U.S. Ambassador

to Thailand Glyn T. Davies. "This new urgency is very welcome."

More than one million children are exploited each year in the global commercial sex trade.

Davies explained that trafficking is a "huge problem in Thailand, as it is in many countries." But the Thai government has shown a "new eagerness" to address the problem and to seek help from the United States, the ambassador said. "That is terrific, because we've got the FBI, the Department of Homeland Security, and the State Department's expertise and resources that we can bring to bear."

Among recent promising developments:

- The Thai government opened a Child Advocacy Center in Chiang Mai, the first of its kind anywhere in Southeast Asia. Based on U.S. models, the center provides shelter and resources for young victims of sexual exploitation and other abuse, and allows specially trained experts to conduct interviews with the

children in a friendly, stress-free environment.

- A law enacted in 2015 has made it easier to arrest and prosecute pedophiles and other sexual abusers who are in possession of child pornography.
- The establishment of the Thailand Internet Crimes Against Children Task Force (TICAC). Based on a U.S. model, the task force combats sexual exploitation facilitated online through shared intelligence. Thai law enforcement officials have recently begun working directly with the National Center for Missing & Exploited Children in the U.S. to share real-time information.
- With training and support from the FBI and Homeland Security Investigations (HSI), an investigative arm of the Department of Homeland Security, the Royal Thai Police is in the process of establishing a victim assistance program—similar to the FBI's Office for Victim Assistance—in which trained police specialists work on behalf of child victims.

Many of these efforts to stem the tide of human trafficking and child sexual exploitation in Thailand have occurred because of the continuing collaboration between Thai law enforcement and U.S. agencies working in Southeast Asia—notably the FBI, HSI, and the U.S. Department of State.

"American law enforcement has been long-time good friends to the Royal Thai Police," said Gen. Tamesak Wicharaya, an assistant commissioner on the police force who oversees the TICAC and has been instrumental in moving the victim assistance program forward.

“Trafficking is a serious crime,” he said. “It is a crime against human dignity, but when they do this to our children, it is even worse.” The general explained that there is a “clear national agenda” in Thailand to address these issues and to assist young people who are sexually exploited by Thai citizens as well as foreign visitors.

“For victims of crime to know that the police force is on their side from day one is very important.”

“We see a large number of travelers from the U.S. and other countries coming here to commit acts against children,” said Special Agent John Schachnovsky, head of the FBI’s legal attaché office in Bangkok. “To travel from the U.S. to any foreign country and engage in sex with a minor is against the law.”

“For victims of crime to know that the police force is on their side from day one is very important,” he said. “The world knows that the sexual exploitation of children is a problem. There aren’t two sides to the issue of taking care of victims. This is a situation where we are able to do something that is 100 percent right.”

Schachnovsky pointed out that providing assistance to victims—as the FBI has formally done since 2001—is not only the right thing to do morally, it helps law enforcement more effectively investigate cases. That, in turn, increases the likelihood abusers will be jailed and will cease to pose a threat to the community.

The more child sex tourists and traffickers who are sent to Thai prisons or returned to the U.S. for



prosecution, said Gen. Tamesak, the more the word goes out that Thailand is no longer a playground for pedophiles and other sexual predators. “We hope that we can send a clear message to those people that Thailand is not a safe haven for them. We will work harder to stop these kinds of people.”

Ambassador Davies agreed. Given the changes taking place from the top down in the Thai government and in law enforcement, he said, “I think people are making a big mistake if they think they can

come here and operate freely when it comes to these types of heinous crimes.”

About This Series

The FBI and other U.S. federal agencies are working closely with the government of Thailand and the Royal Thai Police to fight the scourge of human trafficking and the child sex trade in Southeast Asia. FBI.gov chronicles the efforts in a four-part series called *Report from Thailand*.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/reportfromthailand1.

Child Sex Tourism

Child sex tourism describes the act of traveling to another country to engage in illegal sexual conduct with children. It’s a growing problem thanks to the ease of international travel and the free exchange of information online regarding how and where to find child victims overseas. Children from poor and developing countries are often seen as easy targets by American sexual predators.

The U.S. Department of State estimates that more than a million children are exploited each year in the global commercial sex trade—and that exploitation is illegal. American citizens who engage in sexual contact with a minor overseas are subject to prosecution under various U.S. laws, and those laws were strengthened in 2003 with the passage of the federal PROTECT Act. The law enhances the ability to prosecute and incarcerate individuals who victimize children and removes any statute of limitation on crimes involving the abduction or physical or sexual abuse of a child.

The FBI’s Child Sex Tourism Initiative was established in 2008 to address these crimes and to provide child victims with support and services. Working with state and federal partners, along with foreign law enforcement and non-governmental organizations, the Bureau is actively engaged in investigating and prosecuting American child sex tourists anywhere in the world.

Report from Thailand

Part 2: A New Emphasis on Helping Child Victims



Members of the Royal Thai Police along with personnel from non-governmental organizations gathered in Thailand last April for FBI training focused on human trafficking, the sexual exploitation of children, and how to better assist victims of these crimes. Such a victim-centered approach has become “very important in the U.S.,” said Special Agent Ernie Weyand (right), the assistant legal attaché in the FBI’s Bangkok office who helped organize the training. Specialists from the FBI’s Office for Victim Assistance conducted the training and are helping Thai authorities establish their own victim assistance program.

Generals from the Royal Thai Police—among the highest-ranking officers in the 230,000-member national force—gathered recently in Bangkok for FBI training regarding child victims of trafficking and sexual exploitation. The message they received was simple but powerful: Helping victims is the right thing to do, and it makes it easier to put their abusers behind bars.

Child victims who receive support and assistance from law enforcement are more likely to provide better information to investigators and more willing to make the difficult decision to testify against their attackers in court, increasing the likelihood of successful prosecutions.

The Thai police leaders were among more than 100 members of law enforcement and non-governmental organizations who received training from experts with the FBI’s Office for Victim Assistance. The Thai government requested the FBI’s guidance and support to establish its own victim assistance program.

“The idea of victim assistance is new to the Royal Thai Police,” said Major Gen. Monthon Ngernwattanam, who participated in the training, “but it’s very helpful. This program will show the international community that we can try our best to fight against human trafficking.”

For the FBI, a victim-centered approach in crimes against children cases is standard practice. Victim specialists are on hand during investigations to assist young victims in a variety of ways. Trafficked children might only have the clothes on their backs when recovered by law enforcement. They might live on the street and need shelter, or their parents or caregivers might be their abusers. Victims often need referrals for medical or mental health treatment. They also need an advocate for court proceedings. Just as important, they need adults in their lives who are trustworthy. Victim specialists can provide all those things—and that frees investigators to focus on gathering evidence and preparing cases for prosecution.

“This approach is very important in the U.S.,” said Special Agent Ernie Weyand, the assistant legal attaché in the FBI’s Bangkok office, “but it’s a concept that’s relatively new.” As little as two decades ago, he explained, U.S. investigators “sometimes ran past the victim to work the case, and often the victim was left in the wake.” It was not until the FBI established its victim assistance program in 2001 that things began to change. Today, dedicated victim specialists are assigned to every FBI field office around the country. That is the model the Royal Thai Police seeks to emulate.

“Ultimately that approach made for better cases and made our victims more whole,” Weyand said. “In the end, victims were better—they were better witnesses and they were more complete people. They weren’t harmed in the process of being actively involved in an investigation.”

While the Thai police force works to establish its own victim assistance program, the Child Advocacy Center (CAC)—the country’s first such facility—is already putting the victim-centered concept to work. Located in Chiang Mai, a popular tourist destination in Northern Thailand, the recently opened center offers shelter and resources to victims of child sexual exploitation and other abuses, some as young as 12 years old.

The director of the CAC, who goes by the name Boom, said the center aims to be a “one-stop shop” for victims. “Many of the children here come from poor families,” she said. “They do not have access to counselors or lawyers. We are here to make sure they get all that, along with after-school programs

and basics such as food. We look after them.”

At the same time, the children can establish relationships of trust with investigators in a friendly, stress-free atmosphere away from the sometimes intimidating environment of a police station. “The police are here working with the victims from the beginning,” Boom said.

“The abuse happened, but this place makes sure the kids are not walking alone.”

The center also has an FBI-funded interview room with state-of-the-art recording equipment where trained child forensic interviewers can conduct victim interviews—often a critical part of a sexual exploitation investigation. The recording equipment allows investigators and others such as social workers and prosecutors to view the interview in a separate room as it occurs. That way, young abuse victims are

not re-traumatized by having to tell their story multiple times.

“The CAC offers help and hope,” Boom said. “The abuse happened, but this place makes sure the kids are not walking alone.”

It is hoped that the CAC will serve as a model for more child advocacy centers in Thailand and Southeast Asia. Failing to provide such support and services, said a veteran police detective in Chiang Mai who works with the CAC, will only perpetuate the cycle of abuse.

Without intervention, he explained, young victims may well grow up to become abusers themselves. And abusers can easily become traffickers. “We have experienced many cases of that,” he said. “This is the situation that we have seen.”

With regard to trafficking and the sexual exploitation of children, Weyand noted, “We are all invested in improving what’s happening in Thailand. As the victim-centered approach takes



Boom, the director of the Child Advocacy Center in Chiang Mai.

hold and as victims gain more trust and confidence in the system, I think you are going to see, like we did in the U.S., a tremendous response and a greater number of these cases being investigated and prosecuted, and victims really feeling like they received justice through the process.”



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/reportfromthailand2.

Training for the Future

The three-day Victim Support Services Conference presented in Bangkok this spring to top Royal Thai Police officers—and other victim-assistance training conducted in Thailand—was provided by the FBI’s Office for Victim Assistance and funded through an arm of the U.S. Department of State called the Bureau of International Narcotics and Law Enforcement Affairs (INL).

INL funds a variety of training programs for prosecutors, judges, and law enforcement officials around the world. “In Thailand,” said Rick Snelsire, INL director at the U.S. Embassy in Bangkok, “most of our programs recently have been focused on trafficking in persons—both labor and sex trafficking—which is a big issue here.”

“The Thai government is engaged on this issue,” Snelsire said, explaining that government officials approached embassy and FBI personnel about establishing a victim assistance organization similar to the Bureau’s successful program.

The training conducted in April 2016 represents the first step in the overall plan. Phase one provided senior Thai police leaders with an overview of what a victim assistance program entails and how it could be implemented throughout the police force.

“The next phase will actually be to meet and work with the officers who would be the presumptive victim-witness coordinators at the individual Royal Thai Police stations,” Snelsire said, “and to have FBI personnel on-site to share best practices on how this model works.”

If the program is successful, he added, it could be expanded to include victim-witness coordinators in Thailand’s prosecutors’ offices as well as the police department—as is the U.S. practice.

“We’re really excited,” Snelsire said, “because we are doing something new and innovative that hasn’t been done in this part of the world. We look at Thailand as a kind of a test case for this model. If it works, perhaps we can expand it to other countries in the region—because this problem is not unique to Thailand.”

Report from Thailand

Part 3: It Takes a Village



Left: Sudjai Nakhpian runs the Haven Children's Home in Pattaya, Thailand, a resort town with a reputation as one of the world's leading sex tourism destinations.

On a hot afternoon near the seaside resort town of Pattaya—known as one of the world's leading sex tourism destinations—preteen and teenage boys and girls lounge on the tile floor in a large common room watching a video.

To an uninformed visitor, this might be a day camp or community center. In fact, it is the Haven Children's Home, and the nearly 30 youngsters living at the shelter are all victims of appalling crimes—abandonment, physical abuse, forced labor, sex trafficking.

In most cases, the needs of these children continue long after police arrest those who abused them. The shelter represents one small piece of a larger victim services network that includes law enforcement, the court system, social workers, medical personnel, and non-governmental organizations (NGOs) that provide funding for places like Haven Children's Home.

Through its overseas office in Bangkok, the FBI works with all these groups to further investigations and to help get justice for young victims. Such a multidisciplinary approach—working in tandem with an integrated team of providers—has

proven effective in the U.S. and is increasingly being applied in Thailand. For Sudjai Nakhpian, who runs the Haven Children's Home and has devoted her career to improving the lives of child victims, the concept is a simple one: "We have to help the children," she said, "because the children cannot help themselves. We have to work together."

Thai and migrant children are typically placed at the shelter by the courts. They can range in age from toddlers to teens and can stay as little as a few months or as long as a decade or more. Haven Children's Home is funded by A21, an independent, global non-profit whose mission is to end human trafficking.

"Southeast Asia has one of the highest rates of child trafficking in the world, and, unfortunately, poverty and lack of education makes that possible," said Malina Enlund, A21's Asia director. "The scope of the problem is huge."

Thailand is one of the wealthiest and most developed countries in the region and attracts destitute migrant families from less developed countries such as Laos, Cambodia, and Myanmar. "And of

course, that leads to exploitation," said Enlund, who has worked in Thailand on behalf of trafficking victims for the past eight years.

Exploitation can take the form of children being prostituted or made to work for cheap wages under deplorable conditions. Some migrant parents are so desperate to feed their families that they rent or sell a child to traffickers who send the youngsters out on the street to beg or to work in the sex trade.

"We are talking about thousands of children," Enlund said, and in the case of migrants who have no documentation, they are extremely difficult to help because they are essentially unknown. "If they are trafficked from Cambodia or Myanmar and have no papers," she said, "we are basically looking for children that don't exist."

Thai children, many who live on the street, are also targeted by traffickers and pedophiles from the U.S. and other Western nations. "Right now, Pattaya has one of the largest number of pedophiles anywhere in the world living outside their home countries," Enlund said. And they are not only having sex with children, they are producing child pornography and posting it on the Internet.

Internet forums for pedophiles and pornographers on the so-called Dark Net are expansive and growing, she said, explaining that pedophiles routinely share information online about how to acquire children in Thailand. "With the Internet, we are living in a global community," Enlund said. Pedophiles anywhere are now "five clicks away from finding a

child to abuse. Child sex tourism is growing,” she added. “The demand for children is growing, and it’s being fueled by technology.”

“The demand for children is growing, and it’s being fueled by technology.”

The presence of the FBI, the Department of Homeland Security, and other U.S. law enforcement agencies in Thailand has helped in the fight against child trafficking, Enlund believes. “The U.S. government is the only government I have seen that provides that amount of help to assist children on the ground—and you not only support looking for perpetrators who are American, you also support child sex tourism victims, and that is the only agency that I know of that does that.”

Thai police are trying to do the right thing regarding trafficking investigations and assisting victims, she said, “but I don’t think they are funded enough and I don’t think they are staffed enough.”



As for the Haven Children’s Home, Enlund said, “it is a place where children learn to become whole again. Once they know their boundaries and feel like they are protected within those boundaries, they can thrive and go to school and have a normal life. It’s our hope that we can find families for these kids at some point,” she added. “Every child deserves a family.”

Malina Enlund, Asia director of A21, talks about the challenges posed by child sex trafficking in Thailand and working together with other NGOs, law enforcement agencies, and the Royal Thai Police.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/reportfromthailand3.

Trafficking in Thailand: Signs of Progress

The U.S. Department of State’s annual Trafficking in Persons (TIP) Report is said to be the world’s most comprehensive resource regarding anti-human trafficking efforts. The 2016 report states that while “sex trafficking remains a significant problem in Thailand’s extensive commercial sex industry,” the country is making “significant” progress to deal with its trafficking issues.

“Thailand is a source, destination, and transit country for men, women, and children subjected to forced labor and sex trafficking,” the report said. “Thai victims of trafficking and some of the estimated three to four million migrant workers in Thailand are forced, coerced, or defrauded into labor or sex trafficking.”

The TIP report ranks countries in three tiers according to the seriousness of trafficking offenses and the extent to which governments are addressing the problem. In 2014 and 2015, the report ranked Thailand in the third tier, among the world’s worst offenders. This year’s report marks an improvement, placing the country on the Tier 2 Watch List, noting that while Thailand has “severe forms of trafficking,” it is making “significant efforts.”

Among the TIP report’s recommendations for Thailand:

- Increase efforts to identify victims among vulnerable populations, including migrants, stateless persons, children, and refugees;
- Prosecute and convict traffickers through proactive law enforcement and systematic cooperation with civil society;
- Increase training and resources for multidisciplinary teams; and
- Continue to develop specialized law enforcement and social welfare services for child sex trafficking victims.

Report from Thailand

Part 4: Strengthening Investigations Through Collaboration



As evening falls in Chiang Mai, the street market in the historic district teems with tourists shopping for bargains. Nearby, at one of the city's ancient gates, an open-air park begins to fill with young people. This is where a different kind of commerce occurs.

"Here is where the predator blends into the environment looking for boys and girls for prostitution," said a Royal Thai Police detective who specializes in human trafficking cases and crimes against children. The veteran investigator, who has seen victims as young as 8 years old, explained that while most sex offenders in the West carry out their illicit activity sitting behind a computer, "this is where they come for real. They are hunting children here for real. This is where demand and supply meet."

In Thailand's recent past, it was often difficult to prosecute these offenders because Thai law requires a victim to come forward. Where no victim could be identified or was willing to make a complaint, charges were dropped or never filed. "No victim, no case," the detective said.

But the passage of a law that took effect in late 2015 criminalizing the possession

of child pornography "closed a pretty important loophole," said Rob Abrams, deputy attaché for Homeland Security Investigations (HSI)—an investigative arm of the Department of Homeland Security—at the U.S. Embassy in Bangkok. HSI and FBI investigators work closely together and with Thai law enforcement on human trafficking and child exploitation cases involving U.S. subjects and welcome the new law.

"They are hunting children here for real. This is where demand and supply meet."

"It's a tool that makes it easier to arrest the bad guy," the Chiang Mai detective said, explaining that many sex tourists have child pornography in their possession, either on a smartphone, laptop, or some other device. Rather than having the child victim suffer the trauma of the legal process, he added, "the new law allows the digital evidence to speak for the kids."

The anti-pornography law also benefits the Thailand Internet Crimes Against Children Task Force (TICAC). Newly established with assistance from the FBI and

HSI, the TICAC combats sexual exploitation through shared intelligence.

"What the TICAC has been able to do," Abrams said, "is to leverage this newfound legislative law enforcement authority to go after those who produce child pornography and who commit domestic and international sex trafficking."

Modeled on the American Internet Crimes Against Children Task Force, the TICAC is administered by the Royal Thai Police and includes personnel from other Thai law enforcement such as the Department of Special Investigations, an arm of the Ministry of Justice. A multidisciplinary group of prosecutors and social service organizations are also part of the team.

"The task force acts as a clearinghouse of information related to Internet-facilitated crimes against children," Abrams said, noting that the FBI and HSI have arranged for task force leaders to visit the U.S. to learn American investigative methods and view operations firsthand. "We are very proud, both at HSI and the FBI, of being able to collaborate



Left: Rob Abrams, deputy attaché for Homeland Security Investigations, says that by improving the treatment of victims and witnesses, law enforcement agencies will develop stronger cases. Right: Col. Thakoon Nimsomboon, Royal Thai Police

with our Thai partners on this,” he added. “The enthusiasm from our Thai counterparts has been extraordinary.”

“We are putting a lot more effort into protecting children than in the past. We are working really hard to save children from exploitation.”

Royal Thai Police Col. Thakoon Nimsomboon, who runs the task force’s daily operations, said the FBI and HSI have helped pave the way for the task force to receive real-time cyber tips related to Thailand directly from

the National Center for Missing & Exploited Children, a U.S. organization that works closely with American law enforcement agencies. “We are putting a lot more effort into protecting children than in the past,” the colonel said. “We are working really hard to save children from exploitation.”

“The Thais are developing methods and protocols and defining their technique on how they deal with child exploitation and sex tourism,” said Ernie Weyand, the FBI’s assistant legal attaché in Bangkok. “They are really trying to take international best practice and implement it in their investigations.”

The Chiang Mai detective who has been investigating crimes against children for more than a decade believes the Thai police partnership with American law enforcement has been “a remarkable success. We can run a parallel investigation and not only get the bad guy arrested and prosecuted here, we can also potentially prosecute him in



America. That is a great benefit,” he said. “It brings justice to the victims.”

The end result of the strong collaboration between Thai and American law enforcement means more successful investigations.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/reportfromthailand4.

Internet Crimes Against Children Task Force

The Thailand Internet Crimes Against Children Task Force (TICAC) is modeled on U.S. task forces that have proven highly effective.

An April 2016 report to Congress by the Department of Justice notes a few of the accomplishments of the FBI-led Internet Crimes Against Children Task Force Program:

- It has facilitated the training of more than 500,000 law enforcement professionals since its inception, providing valuable techniques related to investigating, prosecuting, and preventing technology-enabled crimes against children.
- In 2015, 61 coordinated task forces representing more than 3,500 federal, state, local, and tribal law enforcement and prosecutorial agencies conducted more than 54,000 investigations that resulted in the arrest of more than 8,500 individuals.

The report, *The National Strategy for Child Exploitation Prevention and Interdiction*, contains an introduction by Attorney General Loretta Lynch that states, in part: “No matter what form child exploitation takes—from the creation and circulation of child pornography to the trafficking of children for sex—it demands the full attention of law enforcement, policymakers, community leaders, and service providers, each of whom plays an essential role in combating this unconscionable crime.”

Hazardous Devices School

FBI Takes Lead Role in Training Nation's Public Safety Bomb Technicians



Left: FBI Deputy Director Andrew McCabe (center) was on hand at Redstone Arsenal in Huntsville, Alabama for the transition ceremony in which the FBI assumed primary responsibility for the Hazardous Devices School. Also participating from the Bureau were John Selleck, deputy assistant director for the Critical Incident Response Group (left), and Jeff Warren, director of the Hazardous Devices School.

After a 45-year partnership with the U.S. Army, the FBI formally accepted primary responsibility for the Hazardous Devices School at Redstone Arsenal in Huntsville, Alabama, the facility that trains and certifies every one of the nation's public safety bomb technicians.

The transition of responsibility ceremony, which occurred September 21—less than a week after homemade bombs exploded in New York and New Jersey, injuring 29 people—underscores the critical role the Hazardous Devices School (HDS) plays in the country's national security. Some of the unexploded devices in last weekend's incident were rendered safe by local bomb techs who received their training at the HDS.

"The bombing events in New York and New Jersey are a testament to the challenges faced by bomb technicians daily—and an unfortunate reminder of a threat that is both evolving and enduring," noted FBI Deputy Director Andrew McCabe, who was on hand at Redstone Arsenal for the transition ceremony along with other Bureau and Army officials.

McCabe explained that the FBI has an obligation to provide "the best possible tools and training" to local, state, and federal bomb technicians and that the Bureau plans to significantly expand and upgrade the HDS facility over the next several years. The expansion will include state of the art facilities and equipment, he said, to ensure that the HDS "remains the nation's single source of certified training for bomb technicians."

"We have to provide the very best training available. This is a no-fail mission."

Established in 1971, the HDS has provided training to more than 20,000 local, state, and federal first responders and bomb techs. Currently the school trains and certifies approximately 200 new bomb techs each year from the 467 public safety bomb squads around the country, according to the school's director, Special Agent Jeff Warren. The basic certification course provides six weeks of instruction, and each of the country's 3,100 public safety bomb techs—which does not include

the military's explosive ordnance disposal (EOD) technicians—is required to be recertified at HDS every three years.

At the facility's sprawling campus, training is provided in classrooms, explosives ranges, and in "villages" that include mock stores, churches, and apartment complexes that are designed to resemble the conditions bomb techs would face during life or death situations in the real world. In addition to certification and recertification programs, the school offers advance training in a variety of areas, including weapons of mass destruction and electronic and maritime countermeasures.

"The threat from terrorists and other criminals is ever changing," Warren said, and now that the FBI has assumed primary leadership of the HDS, there is a greater responsibility on the Bureau to make sure the nation's public safety bomb techs are prepared for whatever they might face in real life. "We have to provide the very best training available," he said. "This is a no-fail mission."

Although yesterday's ceremony completed the transition of the HDS to the Bureau, McCabe pointed out that the Army will continue to play an important role in the school's mission, "and the FBI looks forward to our continued partnership with the Army and the team at Redstone."

Latest Crime Statistics Released

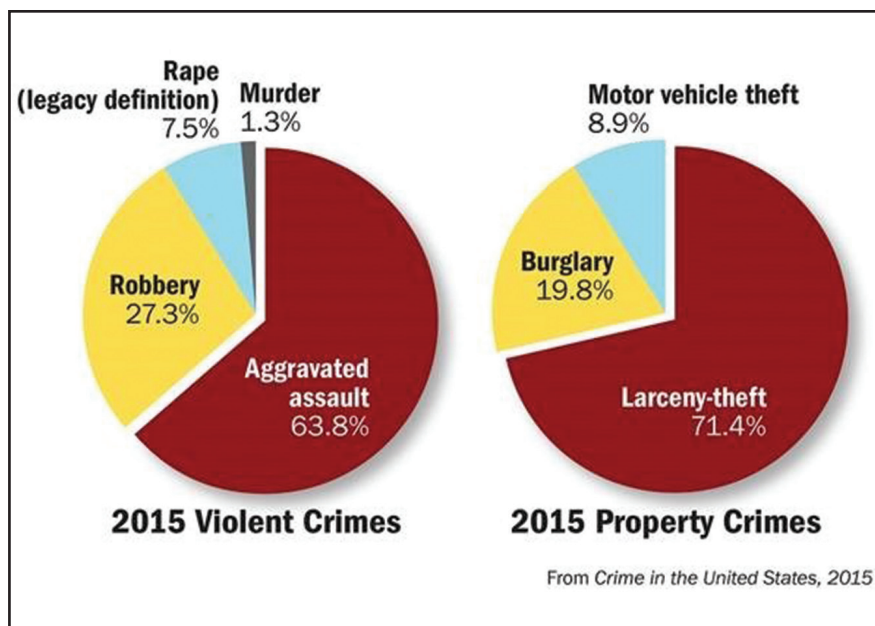
Increase in Violent Crime, Decrease in Property Crime

Today, the FBI released its annual compilation of crimes reported to its Uniform Crime Reporting (UCR) Program by law enforcement agencies from around the nation. *Crime in the United States, 2015* reveals a 3.9 percent increase in the estimated number of violent crimes and a 2.6 percent decrease in the estimated number of property crimes last year when compared to 2014 data.

According to the report, there were an estimated 1,197,704 violent crimes committed around the nation. While that was an increase from 2014 figures, the 2015 violent crime total was 0.7 percent lower than the 2011 level and 16.5 percent below the 2006 level.

Among some of the other statistics contained in *Crime in the United States, 2015*:

- The estimated number of murders in the nation was 15,696.
- During the year, there were an estimated 90,185 rapes. (This figure currently reflects UCR's legacy definition.)
- There were an estimated 327,374 robberies nationwide, which accounted for an estimated \$390 million in losses (average dollar value of stolen property per reported robbery was \$1,190).
- Firearms were used in 71.5 percent of the nation's murders, 40.8 percent of robberies, and 24.2 percent of aggravated assaults.
- Property crimes resulted in losses estimated at \$14.3 billion. The total value of reported stolen property (i.e., currency, jewelry, motor vehicles, electronics, firearms) was \$12,420,364,454.



In addition to national crime data, the publication also contains agency-level data, regional data, state totals, data from cities and counties grouped by populations, and statistics from certain metropolitan areas.

Crime in the United States, 2015 also features several smaller reports:

- Federal Crime Data, the second report from UCR looking at crime reporting from federal agencies, includes 2015 data from FBI and ATF cases as well as traditional offense information from other federal agencies.
- Human Trafficking, the third report from UCR's Human Trafficking data collection, includes general content about human trafficking as well as data provided by agencies that reported human trafficking offenses in 2015.
- Cargo Theft, the third report from UCR's Cargo Theft data collection, contains general information about cargo theft and data provided by agencies that reported cargo theft violations during 2015.

Also included in *Crime in the United States, 2015* is a message from Director James Comey on FBI efforts to improve the collection, analysis, and uses of crime statistics and data about law enforcement's use of force, primarily through its ongoing shift to the more detailed National Incident-Based Reporting System (NIBRS) and a use-of-force database. Both, he said, will "give us a more complete, richer picture of crime in our communities, and a national and detailed picture of the ways we in law enforcement are using force."

According to Comey, who cited the need for more transparency and accountability in law enforcement, "Information that is accurate, reliable, complete, and timely will help all of us learn where we have problems and how to get better."

Animal Cruelty

Houston ‘Crush’ Cases Were First Under Federal Statute

The sentencing last month of a Houston man for creating and distributing videos depicting the torture and killing of small animals brings to a close the first successful prosecutions under a 2010 federal statute specifically tailored to prohibit so-called “crush” videos.

Brent Justice, 55, was sentenced on August 18 in Houston to nearly five years in prison for making videos that featured a woman mutilating and killing puppies, chickens, and kittens between February 2010 and August 2012. The woman in the videos, Ashley Nicole Richards, 25, originally from Waco but residing in Houston, was also convicted.

The case against co-defendants Justice and Richards highlighted a little-known federal statute—The Animal Crush Video Prohibition Act of 2010—that criminalizes the creation, sale, and marketing of videos depicting cruelty to animals to satisfy a fetish. The law’s enactment followed a Supreme Court ruling in 2010 that struck down a 1999 animal cruelty law that was determined to be too broad and a violation of free speech rights.

Richards pleaded guilty last September to four counts of creating crush videos and one count of distribution, making her conviction the first under the 2010 statute. In the videos, which were distributed online, Richards is scantily clad and wearing a Mardi Gras-type mask while making sexual comments to the camera. Crush videos are part of a fetish subculture, with videos circulating online, often under the guise of ritual sacrifices.

Justice was found guilty in state court last February and sentenced to 50 years in prison. He was found

convicted in May on the federal charges and subsequently sentenced to 57 months in prison.

The case was originally investigated by the Houston Police Department, where Officer Suzanne Hollifield followed a tip from the animal rights organization People for the Ethical Treatment of Animals, or PETA.

“I knew what crush videos were, I had been trained to recognize them, but I never expected to see something like that in my career,” said Hollifield, a 22-year police veteran who served on her department’s animal cruelty squad. She quickly identified Richards and Justice in the videos, charging the pair under state animal cruelty laws. The hardest part of the case, she recalled, was reviewing—repeatedly—the horrific videos in order to identify Justice as the camera operator shooting and assisting Richards.

Hollifield, who years earlier worked with the FBI on a cyber crimes task force, sent the digital evidence to the FBI’s Regional Computer Forensics Laboratory (RCFL) in Houston. Federal prosecutors determined the case met the threshold for the 2010 animal crush statute. And the FBI began following the videos’ digital breadcrumbs, investigating the scope of the business venture, which had Internet-based customers across the U.S. and as far away as Pakistan and Italy.

“They were corresponding with people around the world and selling these videos,” said Special Agent David Ko, who was on the Houston FBI’s violent crime squad at the time. “They would ask Richards to put on certain clothing and perform certain acts and send her

money. And then she would buy a certain animal and torture and kill it.”

Evidence presented in court included e-mail correspondence with customers containing links to download the video files and thanking them for wiring money transactions. One e-mail dated August 10, 2012 also included a link to a sample video of a dog being slaughtered.

“It is very cruel video with lots of action and sexy scenes you will like,” the e-mail stated. “Let me know if you like it and what you can afford.”

Richards was sentenced on state charges in 2014 to 10 years in prison. As part of her plea to the federal charges last year, she agreed to testify against Brent Justice.

Prosecutors showed that Justice handled the business side of the video venture, advertising and promoting the underground business, while Richards served as his performer. During his trial, one of the crush videos was played in open court.

“It’s extremely violent. It’s tough to watch,” said Ko, who reviewed more than 16 hours of video to prepare for the original grand jury indictments in 2012. “It’s gratifying to know they’re arrested, behind bars, and not doing these types of crimes anymore.”

“I am very satisfied with the results,” said Hollifield. “It was so horrific. We were determined from the outset to make this case.”

Team USA Athletes Welcomed by FBI

Bureau Holds Career Information Session for Olympians and Paralympians

For some U.S. Olympic and Paralympic athletes, choosing a full-time career path will be their next challenge now that they've returned home from the 2016 Summer Olympic Games in Rio de Janeiro. The FBI intends to make that process easier through a hiring initiative that introduces athletes to job opportunities at the Bureau.

More than 70 Team USA members visited FBI Headquarters in Washington, D.C., Saturday to learn how their athletic and educational experiences could be applied to positions at the FBI. Special agents, intelligence analysts, and human resources specialists were all on hand to share the variety of options currently open to prospective candidates.

The October 1 visit began with opening remarks from Associate Deputy Director David Bowdich, who highlighted the FBI's mission and core values and stressed the importance of maintaining a diverse workforce.

"We need to do everything we can in our power to mirror our country, and we're taking great strides to diversify to the best of our ability," said Bowdich. "It will make us more effective as an organization."

While Saturday morning's visit was the first time the FBI has welcomed such a large group of Olympians and Paralympians to its Headquarters, recruiting dedicated athletes to join the workforce is nothing new for the Bureau. Special Agent Jason Read, for example, continues to train with and compete on the U.S. men's rowing team when he isn't supporting investigations out of the FBI's New York Field Office. In addition to winning several medals in rowing races around the globe,



Associate Deputy Director David Bowdich speaks to U.S. Olympic and Paralympic athletes during a career information session at FBI Headquarters in Washington, D.C., on October 1, 2016. The Bureau hosted the event for athletes interested in pursuing full-time careers following the 2016 Summer Olympics in Rio de Janeiro.

Read counts a gold medal from the 2004 Athens Summer Olympics among his accomplishments.

"The athletic passion on display at the games in Rio can be directly applied to the shared commitment of working for the FBI and keeping our country safe."

Read shared his path from Olympian to special agent and described how he was able to translate his learned dedication and teamwork mantra to being a member of the FBI.

"It was an honor to host fellow Olympians at FBI Headquarters as they begin to research and consider new careers," Read said. "The athletic passion on display at the games in Rio can be directly applied to the shared commitment of working for the FBI and keeping our country safe."

Attendees at the recruiting event represented a cross-section of Olympic teams, including synchronized swimming, shooting, diving, soccer, and rowing. U.S. women's national field hockey team member Kathleen Sharkey joined fellow teammates in touring Headquarters and taking part in the recruiting information session.

"It was interesting to hear about the FBI culture and all the job opportunities there were," Sharkey said. "Coming from a team sport myself, I would thrive and enjoy working in this type of environment."

Like many of her fellow Olympians, Sharkey is now back at home considering what her next steps are going to be now that the Summer Games are over. As the FBI continues to partner with organizations like the U.S. Olympic Committee on its recruiting initiatives, dedicated athletes across the country can find a new home working alongside a motivated team of public servants.

National Cyber Security Awareness Month

Cyber Security is Everyone's Responsibility



Data breaches resulting in the compromise of personally identifiable information of thousands of Americans. Intrusions into financial, corporate, and government networks. Complex financial schemes committed by sophisticated cyber criminals against businesses and the public in general.

These are just a few examples of crimes perpetrated online over the past year or so, and part of the reason why Director James Comey, testifying before Congress last week, said that “the pervasiveness of the cyber threat is such that the FBI and other intelligence, military, homeland security, and law enforcement agencies across the government view cyber security and cyber attacks as a top priority.” The FBI, according to Comey, targets the most dangerous malicious cyber activity—high-level intrusions by state-sponsored hackers and global cyber syndicates, and the most prolific botnets. And in doing so, we work collaboratively with our domestic and international partners and the private sector.

But it's important for individuals, businesses, and others to be involved in their own cyber security. And National Cyber Security Awareness Month—a Department of Homeland Security-administered campaign held every October—is perhaps the most appropriate time to reflect on the

universe of cyber threats and on doing your part to secure your own devices, networks, and data.

What are some of the more prolific cyber threats we're currently facing?

Ransomware is type of malware that infects computers and restricts users' access to their files or threatens the permanent destruction of their information unless a ransom is paid. In addition to individual users, ransomware has infected entities such as schools, hospitals, and police departments. The actors behind these sophisticated schemes advise the users that if they pay the ransom, they will receive the private key needed to decrypt the files. Most recently, these cyber criminals—demonstrating some business savvy—give victims the option of decrypting one file for free to prove that they have the ability to restore the locked files.

Business e-mail compromise (BEC) scams continue to impact many businesses across the U.S. and abroad. BEC is a type of payment fraud that involves the compromise of legitimate business e-mail accounts—often belonging to either the chief executive officer or the chief financial officer—for the purpose of conducting unauthorized wire transfers. After compromising a company's e-mail account—usually through social engineering or malware—the criminals are then able to send wire transfer instructions using

the victim's e-mail or a spoofed e-mail account. BEC scams have been reported in all 50 states and in 100 countries and have caused estimated losses of more than \$3 billion worldwide.

Intellectual property theft involves robbing individuals or companies of their ideas, inventions, and creative expressions—often stolen when computers and networks are accessed by unscrupulous competitors, hackers, and other criminals. Intellectual property can include everything from trade secrets and proprietary products and parts to movies, music, and software. And the enforcement of laws protecting intellectual property rights (IPR)—which are critical to protecting the U.S. economy, our national security, and the health and safety of the American public—is an FBI criminal priority. The Bureau's IPR focus is the theft of trade secrets and infringements on products that can impact consumers' health and safety, including counterfeit aircraft, automotive, and electronic parts.

The FBI is doing everything we possibly can, at every level, to make it harder for cyber criminals to operate,” says Associate Executive Assistant Director David Johnson, “and I believe many of them are now starting to think twice before they put fingers to keyboard. But we also ask that the public do its part by taking precautions and implementing safeguards to protect their own data.”

Check back on our website during the month of October for information on protecting your data and devices and on FBI efforts to combat the most egregious cyber criminals.

National Cyber Security Awareness Month

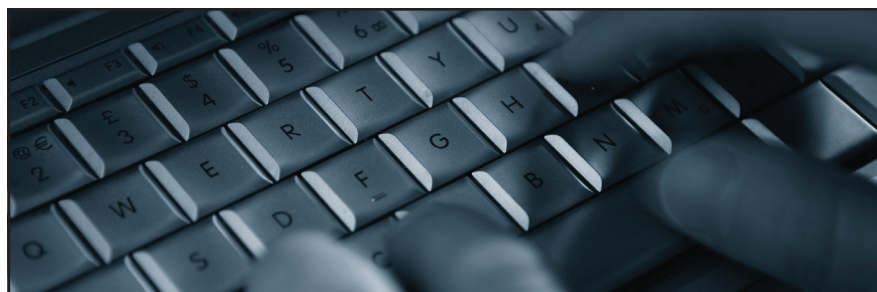
Simple Steps for Internet Safety

In today's digital world, online safety should be of paramount concern for all individuals and organizations because the threats posed by cyber criminals can't be ignored. And to counteract these threats, there are steps you can take to minimize the risks associated with doing any kind of business online, surfing the Internet, and/or sharing information on social media sites.

The first step to greater Internet safety is a basic yet vital one—change online passwords several times a year. Use different passwords for each online account, and make them unique but not easily guessed.

Additional levels of cyber security, like two-factor authentication (TFA), can provide even greater protection for your information. TFA is a technology that increases security by incorporating requirements beyond a password, like a particular physical trait, a dynamic PIN, or the location or time of a login attempt. Many e-mail service providers and social media platforms offer TFA as a free service—most require a strong password and supply a PIN that changes periodically. Users can receive these PINs easily via mobile applications or text messages.

In terms of social media, remember that once personal or organizational information has been posted to a social networking site, that information can no longer be considered private and can be—and sometimes is—used for criminal purposes. The highest security settings on an Internet account may not be enough to prevent a leak of sensitive data—for example, cyber criminals often can obtain personal passwords regardless of their complexity. In



doing so, they can gain access to banking credentials and credit card numbers, get hold of social security information, download malware to a computer, or hijack a device to perpetrate further crimes. So be careful—post as little personal information as possible, use two-factor authentication, and beware of embedded links that—if clicked on—may lead to scam webpages and malware being downloaded to your computer or mobile device.

Another level of online security involves protecting your mobile devices from cyber intruders in public places. Not all WiFi hotspots at coffee shops, airports, or hotels have strong security protections. Persons in close proximity may be able to access that open network and collect your login information and the content of your online browsing. Securing your phone or tablet is as simple as avoiding sensitive sites that require a login, so try to avoid signing into bank accounts, e-mail, or social media accounts while on a public WiFi hotspot. But if you have to, use a reliable personal virtual private network (VPN) service provider. A VPN enables data encryption and adds a layer of security to communications, making it more difficult for cyber criminals to spy on you.

An out-of-band backup is another useful cyber security technique. This involves backing up your data

to a virtual, cloud environment or storing hard copies of digital data at a physical location elsewhere. Using this method is ideal in combating ransomware, a type of malware which restricts access to files or threatens their destruction unless a ransom is paid to the cyber-based

Kids too can learn steps to Internet safety through the FBI's Safe Online Surfing (SOS) program. SOS is a nationwide initiative designed to educate children from grades 3 to 8 about the dangers faced when surfing the web. SOS promotes good cyber citizenship among students by engaging them in a fun, age-appropriate, competitive online program where they learn how to safely and responsibly use the Internet.

Though myriad methods and tools exist to protect the public and organizations from the risks of cyber crime, your best defense is understanding and implementing strong security practices and maintaining them regularly. Doing so can raise a perpetual firewall against cyber criminals and keep your sensitive data safe.



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/ncsam2016

Operation Cross Country X

Recovering Underage Victims of Sex Trafficking and Prostitution



Left: FBI Director James Comey, along with law enforcement partners, announces the results of Operation Cross Country X at a press conference in San Diego, California on October 17, 2016. Bottom Left: In Detroit, an FBI agent takes a suspected pimp into custody. Bottom right: Overseas, Thai police officers monitor a sting operation as part of the three-day law enforcement action. In the U.S., Operation Cross Country X resulted in the recovery of 82 adolescent victims and the arrest of 239 pimps and other individuals.

other areas frequented by pimps, prostitutes, and their customers. The youngest recovered U.S. victim was 13 years old.

All of the recovered U.S. minors were offered services by victim specialists who are part of the FBI's Office for Victim Assistance. More than 100 victim specialists provided on-scene services that included crisis intervention as well as resources for basic needs such as food, clothing, shelter, and medical attention.

“...there are people who spend every day worrying about how to rescue these children. They are true heroes.”

Among the 82 juveniles recovered in the U.S. were two sisters in Milwaukee, ages 16 and 17, who told authorities that their mother was their pimp. The girls said their mother also rented out their brother's room to a man who was a registered sex offender.

Working with the FBI's legal attaché offices, international law enforcement partners conducted their own operations. In Thailand, authorities arrested an American citizen—a registered sex offender—after he coerced five Filipino girls, ages 14 to 16, to take sexually explicit photos of themselves and send them to him online. In

Operation Cross Country, the FBI's annual law enforcement action focused on recovering underage victims of prostitution and drawing the public's attention to the problem of sex trafficking at home and abroad, has concluded with the recovery of 82 sexually exploited juveniles and the arrests of 239 pimps and other individuals.

Now in its 10th iteration, Operation Cross Country has expanded to become an international enforcement action, with Canada, Cambodia, the Philippines, and Thailand joining the FBI and its local, state, and federal law enforcement partners—along with the National Center for Missing & Exploited Children (NCMEC)—during the coordinated three-day operation that ended October 16.

“Operation Cross Country aims to shine a spotlight into the darkest

corners of our society that seeks to prey on the most vulnerable of our population,” said FBI Director Comey, announcing the results of the operation during a press conference today in San Diego at the International Association of Chiefs of Police annual gathering. “We are not only looking to root out those who engage in the trafficking of minors, but through our Office for Victim Assistance, we offer a lifeline to minors to help them escape from a virtual prison no person ever deserves.”

This year's Operation Cross Country—the largest to date—involved 55 FBI field offices and 74 FBI-led Child Exploitation Task Forces throughout the country composed of more than 400 law enforcement agencies. Hundreds of law enforcement officials took part in sting operations in hotels, casinos, truck stops, and



Screen capture from raw video (b-roll)
footage of Operation Cross Country X.

the Philippines, two boys, ages 11 and 5, and a 2-year-old girl were recovered when five adults were arrested for operating a web-streaming service where individuals online paid for access to livestreamed child sexual abuse, as well as access to the children for the purposes of illegal sexual acts.

The Thai case was initiated through a cyber tip to the Royal Thai Police from NCMEC, the U.S. non-profit organization that serves as a resource center and information clearinghouse to help missing and exploited children. NCMEC's work with overseas law enforcement agencies illustrates one example of the international partnerships that have formed to fight child sexual exploitation.

NCMEC's president and CEO, John Clark, noted that the exploitation of children is a serious problem in the U.S. as well as abroad. "This is something that's happening in communities all across the country," he said. "We need moms and dads and teachers

and neighbors and everybody working hand in hand to try to identify where this situation is happening so that we can bring the right resources to bear to fight child sex trafficking."

*"This is something
that's happening
in communities all
across the country."*

Operation Cross Country is part of the FBI's Innocence Lost National Initiative, which began in 2003. Since its creation, the program has resulted in the identification and recovery of more than 6,000 children from child sex trafficking, and prosecutors have obtained 30 life sentences in cases against traffickers and their associates.

The fight against underage trafficking is largely coordinated through the Child Exploitation Task Forces, which are staffed by state, local, tribal, and federal law enforcement personnel who work to identify and prosecute individuals

and criminal enterprises who sexually exploit children. That work is ongoing.

One of the goals of Operation Cross Country is to raise public awareness about the seriousness of child sexual exploitation and how it takes strong partnerships to protect young people from being trafficked, which Comey called a "scourge that spans all our borders."

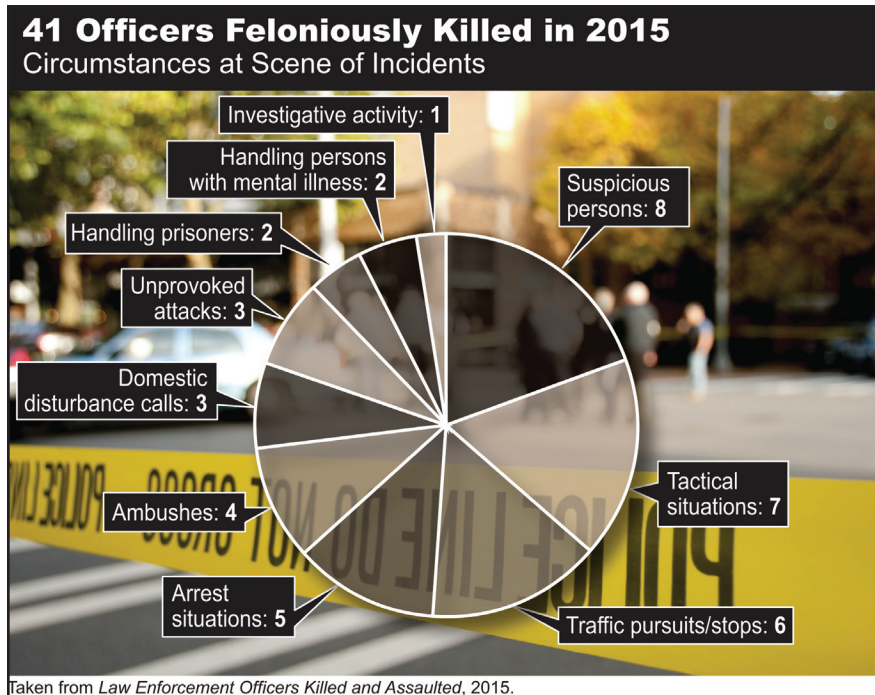
This is a depressing day in law enforcement," Comey said, announcing the number of juveniles who had been rescued, "because this is the world we live in and the work we have to do." But it is also a proud day for law enforcement, he added, "because there are people who spend every day worrying about how to rescue these children. They are true heroes."



Scan this QR code
with your smartphone
to access related
information, or visit
www.fbi.gov/occx.

LEOKA Report Released

41 Officers Feloniously Killed in 2015



Today, the FBI released its annual *Law Enforcement Officers Killed and Assaulted* (LEOKA) report—this one covering the 41 felonious deaths, the 45 accidental deaths, and the 50,212 line-of-duty assaults of officers during 2015.

Among the report's highlights:

- The number of officers killed as a result of criminal acts in 2015—41—decreased from the 2014 figure of 51. The average age of the officers killed feloniously in 2015 was 40, and the average length of service was 12 years.
- Of the 41 officers feloniously killed, 38 were male and three were female. More than half—29—were on vehicle patrol when the incidents happened. Thirty-eight of these 41 officers were killed with firearms, and

30 of those were wearing body armor at the time. For more details on each incident, read the summaries section of the report.

- Motor vehicles played a key role in the deaths of the 45 law enforcement officers accidentally killed in the line of duty—29 were involved in automobile accidents, four were killed in motorcycle accidents, and another seven were struck by vehicles while directing traffic, assisting motorists, executing traffic stops, etc.
- Of the 50,212 officers assaulted while performing their duties in 2015, 14,281 (or 28.4 percent) sustained injuries. And 79 percent of the officers who were assaulted in the line of duty were attacked with personal weapons (such as hands or feet).

Law Enforcement Officers Killed and Assaulted also contains a separate section on federal law enforcement officers who were killed or assaulted in the line of duty during 2015.

Update to LEOKA Program Data Collection

Effective March 23, 2016, the LEOKA Program expanded its data collection to include the data of military and civilian police and law enforcement officers of the Department of Defense (DoD) who are performing a law enforcement function/duty and who are not in a combat or deployed status (sent outside the U.S. to a specific military support role mission). This includes DoD police and law enforcement officers who perform policing and criminal investigative functions while stationed (not deployed) on overseas bases, just as if they were based in the United States. The new information will be contained in the 2016 edition of *Law Enforcement Officers Killed and Assaulted*, which will be released later in 2017. Read more on the criteria used to determine suitability for inclusion in the LEOKA report.

In addition to collecting details about the critical aspects of fatal confrontations and assaults—and sharing that information with our law enforcement partners, government and civic leaders, researchers, and the public in general—the FBI's LEOKA Program conducts extensive research on the data that eventually gets incorporated into officer safety awareness training the Bureau provides.

National Cyber Security Awareness Month

FBI, Partners, Offer Online Cyber Training for Law Enforcement First Responders

Since the advent of the Internet and, more recently, the proliferation of technological gadgets—like cell phones, laptops, tablets, game consoles, even wearable technology—criminals of all kinds are increasingly leaving behind a trail of digital evidence when committing their crimes.

So it's imperative that law enforcement agencies around the country—in particular, the first responders to a crime scene—have a working knowledge of how to survey and secure electronic evidence in addition to the physical evidence that they're more accustomed to, like fingerprints and DNA.

But being truly effective at securing digital evidence requires an extra level of cyber knowledge. That's why the International Association of Chiefs of Police (IACP)—concerned about the lack of affordable basic cyber training for officers in mostly smaller and some mid-size police agencies—contacted the FBI and asked for assistance. And in response, the FBI's Cyber Division—with the IACP and cyber experts from Carnegie Mellon University in Pittsburgh—developed the Cyber Investigator Certification Program (CICP). This self-guided, online training program is now available—free of charge—to all local, state, tribal, territorial, and federal law enforcement personnel.

CICP's inaugural course, launched in October 2015, specifically targets law enforcement first responders. "The goal of the course," explains Special Agent James McDonald from the Cyber Division's Cyber Training and Logistics Unit that oversees CICP, "is to improve a first responder's technical knowledge by focusing on best practices in terms

of investigative methods specific for cyber investigations." He added, "The more first responders understand about technology, the less chance there is of errors being made while securing a crime scene involving digital evidence.

The first responders course—which doesn't have to be taken in one sitting—features nine modules; each one focuses on a particular topic, like software, hardware, the Internet and social networks, encryption, legal tools, and digital evidence. Each of the modules uses a "you are there" style where trainees can see the instructors and follow the presentation as though they were in the classroom. The instructors include top-notch cyber experts from the FBI and Carnegie Mellon, other law enforcement agencies, and prosecutors' offices.

The modules drill down further into each of the topics with everyday information of vital importance to law enforcement first responders. For example:

- The software session includes a primer on such topics as metadata, operating systems, backup systems, apps, Internet communication, and the cloud, while the hardware lesson covers things like specific digital devices, electronic storage, and networks.
- The legal skills training goes into how to conduct search warrants and consent searches involving digital evidence as well the ins and outs of the Electronic Communications Privacy Act.
- The digital evidence module offers instruction on recognizing potential sources of digital evidence, securing a digital device, and documenting the crime scene.

Running throughout the overall training course is a realistic case scenario of a digital crime. The scenario, which makes use of professional quality and engaging videos, focuses on the aspect of the investigation involving first responders. And once the entire training session is completed, the officer receives a course certificate.

This first responders course is just the first one out of the barrel. The FBI and Carnegie Mellon are nearing completion of four cyber training courses (collectively called Level 1) that are designed to be more case specific and target beginning to intermediate-level detectives. These courses will focus on the crimes of digital harassment, online fraud, child enticement, and identity theft, and will also feature case scenarios—based on actual investigations—that highlight best investigative practices for crimes with a cyber angle.

And in the developmental stages are three Level 2 training courses designed for intermediate to advanced detectives to investigate network-based crimes. Some of the topics to be covered will include malware, worms, and viruses.

Nearly 5,000 law enforcement officers have enrolled in the first responders course so far, and we expect that number will continue to grow.

As FBI Director James Comey, who is featured in an introductory video at the beginning of the first responders training, said, "Our collective success in analyzing crime scenes depends upon your ability to both assess and secure an increasing amount of digital artifacts, so it is important that we use best practices in working with digital evidence."

Combating the Growing Money Laundering Threat

Specialized FBI Unit Focuses on Disrupting Professional Money Launderers



Every year, more than \$300 billion in concealed transactions is moved around the United States, according to a U.S. Department of the Treasury report on money laundering and terrorist financing threats.

Transnational criminal organizations, foreign intelligence services, and terrorist groups—as well as Internet fraudsters and other criminals—move billions of dollars each year through the international banking system and across borders to conceal the origin of the funds. To more effectively address the threat, the FBI has placed a renewed emphasis on investigations that target the middlemen who facilitate the hidden flow of cash.

“Our focus is on third-party facilitators,” said James Barnacle, who heads the FBI’s Money Laundering Unit. “They include, among others, lawyers, accountants, and brokers with the ability to facilitate the process of moving money for dangerous criminal organizations. That’s who our targets are.”

The facilitators use traditional and non-traditional means to

launder staggering amounts of illicit proceeds every year. Barnacle said business e-mail compromise, or BEC, scams and the use of virtual currencies are on the rise

To help combat this growing threat, the FBI has been adding resources to its Money Laundering Unit in the Criminal Investigative Division. The team has been intensifying its efforts to support existing investigations and to identify and investigate previously unknown facilitators. It works alongside other Bureau divisions, including Counterintelligence and Cyber, to analyze criminal networks and to disrupt their operations. The team also provides guidance and training and works with domestic and foreign law enforcement partners to develop initiatives that support investigations in the FBI’s 56 field offices.

Innovations in technology have made it easier for launderers to communicate anonymously and move money, making it more challenging to identify, investigate, and prosecute launderers, who shield a staggering amount of money in their varied illegal

transactions. These types of crimes often come to light through tips from within the private sector or the general public.

“One of the tools we use to combat money laundering is the Internet Crime Complaint Center website, or IC3.gov,” said Barnacle. “We encourage victims of fraud to submit a report on the IC3.gov site as soon as possible. It’s a tremendous asset for our team.”

One of the Money Laundering Unit’s most critical partnerships is with the private sector, where financial institutions face significant risks and are required to have robust anti-money laundering policies and procedures.

“The relationship we have with private industry is just as important as the partnerships we have with other government agencies and regulators,” said Barnacle. “Our mission would not succeed without our partnership with the private sector.”

What is Money Laundering?

Money laundering is the process by which criminals conceal or disguise their proceeds and make them appear to have come from legitimate sources.

Money laundering allows criminals to hide and accumulate wealth, avoid prosecution, evade taxes, increase profits through reinvestment, and fund further criminal activity.

While many definitions for money laundering exist, it can be defined very simply as turning “dirty” money into “clean” money. And it’s a significant crime—money laundering can undermine the integrity and stability of financial institutions and systems, discourage foreign investment, and distort international capital flows.

The FBI focuses its efforts on money laundering facilitation, targeting professional money launderers, key facilitators, gatekeepers, and complicit financial institutions, among others.

National Cyber Security Awareness Month

FBI Deploys Cyber Experts to Work Directly with Foreign Partners

Last month, FBI Director James Comey told a congressional committee that “the pervasiveness of the cyber threat is such that the FBI and other intelligence, military, homeland security, and law enforcement agencies across the government view cyber security and cyber attacks as a top priority.”

Operationally, the Bureau is responding to this global threat in a variety of ways—including through our Cyber Threat Team model, the FBI-led National Cyber Investigative Joint Task Force, our Cyber Action Team, and regional cyber task forces in all 56 field offices.

Another way we’re working to combat the cyber threat is by placing Bureau cyber experts in FBI legal attaché (legat) offices in strategic locations around the globe—a critical step because cyber threat actors can and do operate virtually anywhere in the world, crossing national and international borders with a few strokes of a keyboard to reach their victims.

Our experts are called cyber assistant legal attachés, or ALATs, and they work on a daily basis with law enforcement in host countries, sharing information, cooperating on investigations, and enhancing our relationships overall. Sometimes, they even work in the same physical space alongside their foreign counterparts.

The cyber ALAT program began in 2011, when several FBI Cyber Division personnel were deployed to a handful of legat offices to address significant cyber threats in those regions impacting U.S. interests and FBI investigations.

Five years later, there are eight permanent cyber ALAT positions—two in London and



one each Bucharest, Romania; Canberra, Australia; The Hague, Netherlands; Tallinn, Estonia; Kyiv, Ukraine; and Ottawa, Canada. And currently, the Bureau maintains nearly a dozen temporary duty (TDY) cyber ALAT positions—their locations determined by the cyber threat environment and the host nation’s capabilities in working with the FBI in identifying, disrupting, and dismantling cyber threat actors and organizations.

The work of cyber ALATs provides a number of benefits for the Bureau, including improved working relationships with our partners to further FBI investigations and initiatives; assistance with the differences in countries’ jurisdictional issues, cyber laws, and legal processes; and a fuller picture of particular cyber threats.

The host nation also benefits from the presence of a cyber ALAT in the way of technical assistance offered in support of cyber investigations as well as information-sharing efforts that often eliminate the duplication of resources expended to investigate the same threat actor groups. Cyber ALATs can also facilitate requests from our foreign partners for cyber training.

Because of the nature of the work, cyber ALAT positions are highly

competitive. Only those FBI agents with proven leadership skills, a wealth of task force and liaison experience, plenty of initiative, and top-notch computer intrusion knowledge are selected for the permanent and TDY jobs.

When all is said and done, what impact can cyber ALATs actually have on the overall cyber threat picture? “By building relationships, cyber ALATs can identify common threats and find unique opportunities to mitigate those threats with our international partners,” said one recent cyber ALAT. “Historically, law enforcement agencies ask each other to provide specific information to forward domestic investigations. But the global nature of cyber threats requires that the FBI and its foreign partners learn each other’s strengths, priorities, and gaps. Cyber ALATs create the bridge that allows the Bureau and its partners to address both individual cyber cases and global cyber threats with the most impact.”

Our cyber ALAT program is one more tool the FBI is using to protect the nation from sophisticated cyber threats coming from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists.

A Primer on DarkNet Marketplaces

What They are and What Law Enforcement is Doing to Combat Them



Last week, the FBI joined a number of other U.S. law enforcement agencies in Operation Hyperion, a successful international action aimed at disrupting the operations and infrastructure of illicit DarkNet marketplaces.

The initiative was the brainchild of the Five Eyes Law Enforcement Group (FELEG), an international coalition of law enforcement agencies from Australia, Canada, New Zealand, the United Kingdom, and the United States who share criminal intelligence and collaborate on operations to combat transnational crime. FELEG has a number of working

groups that concentrate on specific criminal or functional areas, and one of those groups—the Cyber Crime Working Group—focuses on identifying the sophisticated perpetrators operating key criminal services in the cyber underground marketplace.

But what are these underground marketplaces, and what exactly is the DarkNet? To understand both, you first have to have a basic understanding of the entire Internet.

- First, there's what's known as the Clear Web, or Surface Web, which contains content for the general public that is indexed by

traditional search engines (like websites for news, e-commerce, marketing, collaboration, and social networking). The FBI's own public website is part of the Clear Web.

- But there is a vast amount of web content out there on the Internet, and much of it is not indexed by traditional search engines—that part of the web is known as the Deep Web. Its content is still available to the general public, but it's harder to find unless you have the exact URL. Examples of Deep Web content are websites and forums that require log-ins, websites that don't allow for indexing or

aren't linked to anything, and databases.

- And finally, there's the DarkNet, which is a subset of the Deep Web. DarkNet content is not indexed and consists of overlaying networks that use the public Internet but require unique software, configuration, or authorization to access. And this access is predominately designed to hide the identity of the user.

There is some criminal activity—like fraud schemes—that takes place on the Clear Web and on the Deep Web. And there *are* some legitimate uses—and users—of the DarkNet. But because of the anonymity it offers, many criminals and criminal groups gravitate toward the DarkNet, often doing business through online marketplaces set up for nefarious purposes.

What's available for sale through illicit DarkNet marketplaces? Typically, products and services involve child sexual exploitation; drugs; guns; chemical, biological, and radiological materials and knowledge; stolen goods; counterfeit goods; and computer hacking tools. Payment for these goods and services is usually through virtual currency like bitcoin, also designed to be anonymous.

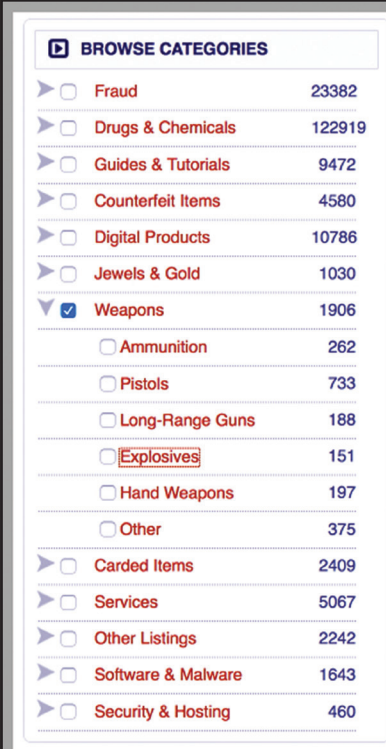
On illicit DarkNet marketplaces—just like on legitimate online marketplaces on the Clear Web—buyers can also provide feedback on products and services, communicate through internal

messaging, and take part in website forums. The difference, of course, is that the feedback, internal messaging, and forums on DarkNet marketplaces focus on topics like the quality of child pornography images, the potency of a particular poison, or the speed at which a cache of guns is mailed to its buyer.

In its investigative efforts against DarkNet marketplaces, the FBI—much like in our other criminal priorities—focuses its resources not on individual criminals but on the most egregious criminal organizations and activities.

Illicit DarkNet marketplaces, by their very nature, are difficult to penetrate. But not impossible. The Bureau, with its partners, uses all available investigative techniques to target buyers, sellers, marketplace administrators, and the technical infrastructure of the marketplaces themselves. And we have had success doing it.

For example, in November 2014, federal law enforcement took action against more than 400 hidden service DarkNet addresses, including dozens of illicit marketplace websites operating on what is known as the Onion Router, or Tor, network, which was designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network. One of the most prolific websites taken down as a result of those investigative activities was Silk Road 2.0—and the website's operator was arrested and charged.



BROWSE CATEGORIES	
<input type="checkbox"/> Fraud	23382
<input type="checkbox"/> Drugs & Chemicals	122919
<input type="checkbox"/> Guides & Tutorials	9472
<input type="checkbox"/> Counterfeit Items	4580
<input type="checkbox"/> Digital Products	10786
<input type="checkbox"/> Jewels & Gold	1030
<input checked="" type="checkbox"/> Weapons	1906
<input type="checkbox"/> Ammunition	262
<input type="checkbox"/> Pistols	733
<input type="checkbox"/> Long-Range Guns	188
<input type="checkbox"/> Explosives	151
<input type="checkbox"/> Hand Weapons	197
<input type="checkbox"/> Other	375
<input type="checkbox"/> Carded Items	2409
<input type="checkbox"/> Services	5067
<input type="checkbox"/> Other Listings	2242
<input type="checkbox"/> Software & Malware	1643
<input type="checkbox"/> Security & Hosting	460

Shown is a screenshot of a listing taken from the website of an illicit DarkNet marketplace featuring the various categories of illegal merchandise that buyers can browse through.

Successes like this are vital. Yes, they allow us to dismantle illicit websites and go after those responsible for them. But they also enable us to develop actionable intelligence on other websites, criminals, and criminal organizations. And the knowledge we gain from these investigations helps us create more sophisticated investigative tools to shine a brighter light into criminal activity on the DarkNet.

More on Operation Hyperion

During Operation Hyperion, FBI agents made contact with more than 150 individuals around the country suspected of purchasing illicit items from various DarkNet marketplaces. Some of these individuals confessed to ordering a range of illegal drugs and controlled substances online, including heroin, cocaine, morphine, and ketamine.

Public Corruption

Chicago Transportation Official Took Bribes for a Decade



John Bills once held a position of trust as Chicago's assistant transportation commissioner. Now the 55-year-old is serving a 10-year prison sentence for his role in a long-running corruption scheme involving the city's red-light camera contracts.

"Chicago has a well-known history of public corruption," said Special Agent Brian Etchell, "but even by Chicago's standards, this case stands out."

That's because the corruption went on for nearly a decade, and "the sheer amount of cash bribes to Bills—more than \$600,000—was stunning," said Etchell, who investigated the case with Special Agent Craig Henderson from the FBI's Chicago Division. Henderson noted that the corruption scheme involved payments and perks that totaled more than \$2 million.

In 2003, Bills served on a committee seeking vendors for the city's Digital Automated Red Light Enforcement Program. That committee recommended awarding contracts to Redflex Traffic Systems, an Arizona company eventually hired to install cameras that automatically recorded and ticketed drivers who ran red lights.

From the time Redflex received the contract in 2003 until Bills retired in 2011, evidence showed that the transportation official used his influence to expand Redflex's business in Chicago. That resulted in millions of dollars in contracts for the installation of hundreds of red-light cameras. Redflex was enriched—and the company made sure Bills was as well.

The company gave Bills cash, expensive meals, golf outings, airline tickets, hotel rooms, and more. Some of the benefits were

given to him directly, while hundreds of thousands of dollars in cash was funneled to Bills through his friend Martin O'Malley, whom Redflex hired to facilitate the payoffs.

As a Redflex contractor, O'Malley was paid lavish bonuses as new cameras continued to be added in the city. O'Malley, in turn, stuffed envelopes full of his bonus cash and gave them to Bills, often during meals in Chicago restaurants. O'Malley also used some of the money to buy and maintain a condo in Arizona that Bills used as his own.

Bills had more cash than he knew what to do with. "He would ask co-workers to purchase airfare tickets on their credit cards," Henderson said, "and then he would repay them on the spot in cash. He had his friends write him personal checks, and then he would



While he was an influential official with Chicago's Department of Transportation, John Bills took hundreds of thousands of dollars in bribes from an Arizona company that was contracted to provide the city with red-light cameras. Through a middleman, the company provided Bills with the use of a luxury condominium in Arizona, shown here in an exhibit presented at his trial.

immediately give them cash—he would just hand over \$3,000 right there.”

When a Redflex employee alleged misconduct regarding how Chicago's red-light camera business was being conducted, the company did an internal investigation and found nothing wrong. Later, after a newspaper exposé raised questions about the relationship between Redflex, O'Malley, and Bills, the company began another inquiry, and information from that investigation was presented to the FBI and the United States Attorney's Office.

“I would like to think that with each of these investigations, we chip away, piece by piece, at this culture of corruption.”

“Based on the company's investigation, we opened a case starting in 2013,” Etchell said. “We were able to establish a direct

link between O'Malley, Bills, and the Arizona condominium. The majority of the bribes were flowing through Redflex to O'Malley to that condominium.”

Etchell and Henderson specialize in public corruption investigations, the FBI's top criminal investigative priority. They painstakingly documented patterns that tied O'Malley's cash withdrawals to purchases by Bills and showed how O'Malley's cash withdrawals coincided with personal meetings with Bills.

Even so, “much of the evidence was still circumstantial,” Henderson said. So the investigators interviewed countless individuals, many of whom worked with Bills and at Redflex. In 2014, O'Malley was arrested. Faced with the mounting evidence against him, he began cooperating with the investigation and laid out the entire scheme.

“He was the middleman, the bagman,” Etchell said, “and he

decided to cooperate with us.” Bills was indicted in 2014. In January 2016, a federal jury convicted Bills on all counts against him, among them mail fraud, wire fraud, bribery, and filing false tax returns. He was sentenced in August 2016. A month later, O'Malley, 75 and in frail health, received a six-month prison term.

Karen Finley, a former CEO of Redflex, pleaded guilty in 2015 to one count of conspiracy to commit bribery in the red-light camera corruption scheme. She awaits sentencing.

Henderson thanked the FBI's law enforcement partners—the Internal Revenue Service, the City of Chicago Office of Inspector General, and the U.S. Attorney's Office—for making “large contributions to the case.” He added, “I would like to think that with each of these investigations, we chip away, piece by piece, at this culture of corruption.”

Burglary Crew

Break-In Netted 'Jedi Knight' Thieves \$2.5 Million in Jewels



The group of friends in their late 20s had known each other since high school and called themselves the “Jedi Knights.” The name was based on the *Star Wars* movie characters who used “the Force” to bring balance and harmony to the universe. These Jedi Knights, however, were more interested in forced entry—as in burglary.

By their own accounts, the robbery crew loosely based in New York state committed several hundred home break-ins up and down the East Coast during 2011 and 2012. In February 2012, two of the Jedi Knights, Jason Gatto and Michael Simpson, chose a modest-looking house in Salisbury, Connecticut, where no one seemed home. They knocked on the front door. If someone answered, the pair, professionally dressed in shirts and ties, would make up a story about why they were there. If no one was home, which was the case—the victim and her husband’s primary residence was in New York City—the plan was to go to the back of the house and break in.

The half-dozen principal members of the burglary crew all had Jedi Knights tattoos on their arms, and the thieves had a code of conduct: All proceeds were split evenly among the group, and members vowed to never snitch if arrested. Their strategy was to steal cash, jewelry, and weapons, and leave just about everything else behind.

Inside the Connecticut home that winter day, Gatto and Simpson discovered a linen closet that contained inexpensive plastic containers—similar to fishing tackle boxes—full of jewelry. Because of the cheap containers and where they were located, the men believed the roughly 250 rings, watches, bracelets, and brooches were fakes. They took the jewelry, but as they drove away from the home, they threw a number of pieces out the car window.

“It was dumb luck that they came up with such a valuable haul. They had never hit the jackpot like they did this time.”

It was only later, after Simpson’s girlfriend and accomplice got a look at the jewelry—pieces made by Cartier, Tiffany, and Van Cleef—that the Jedi Knights began to understand that they had made the heist of their lives.

“It was dumb luck that they came up with such a valuable haul,” said Special Agent Jennifer Berry, who investigated the case from the FBI’s New Haven Division along with the Connecticut State Police. “They had never hit the jackpot like they did this time.”

The total estimated value of the jewels was \$2.5 million. Gatto, Simpson, and Simpson’s girlfriend, Martha Dahl, went to North Carolina with the jewelry, where a fellow Jedi Knight, Miguel Mead, later met them. The pieces were distributed among the group, who began to sell them to pawn shops, fences, and other buyers.

“They sold the jewels in Nevada, California, North Carolina, all over the country,” Berry said, “and

for a fraction of what they were worth—it was pennies on the dollar.” Investigators picked up the Jedi Knights’ trail, Berry explained, when stolen items started turning up. “We were notified when a Cartier watch that belonged to the victim showed up at a pawn shop in Beverly Hills, California.”

That watch led investigators to Dahl, and later to the other members of the burglary crew. In January 2016, Gatto was arrested for his role in the Connecticut robbery, and two months later the Jedi Knights ringleader pleaded guilty to one federal count of conspiracy to transport stolen property.

Eventually, Simpson, Dahl, and Mead also pleaded guilty in connection with their roles in the Connecticut theft. In February 2016, Mead was sentenced to 41 months in prison. In August 2016, Gatto received a 40-month term. Simpson and Dahl await sentencing.

After the burglary, police recovered some of the stolen jewelry that Gatto and Simpson had discarded along Route 41 in Salisbury. But the majority of the pieces were never recovered.

“What’s sad,” Berry said, “is that much of the jewelry had belonged to the victim’s grandmother, and it had tremendous sentimental value.” A one-of-a-kind brooch signed by the artist and valued at \$65,000, for example, was lost forever because the Jedi Knights sold it to a smelter for under \$1,000. “That’s what they did with a lot of the pieces,” Berry said. “They sold them for the weight of the gold and they were melted down.”

A Legacy of Crime Brought to an End

Violent Gang Leader in Buffalo Sentenced for Role in Murders

The 7th Street Gang in Buffalo, New York was once considered one of the most violent criminal organizations in the city. It terrorized the surrounding neighborhood while its leader, Efrain “Cheko” Hidalgo, led a bloody turf war with a rival gang. Murders and shootings were rampant for almost six years before an FBI-led investigation dismantled both gangs and, in August, placed Hidalgo behind bars.

“Hidalgo was a driving force behind the rivalry and all of the violence in the West Side,” said Special Agent Jason Galle, who investigated the case out of the FBI’s Buffalo Field Office. “The evolution from dealing drugs with his street corner gang to becoming the leader of the largest criminal enterprise in the city was rapid.”

“Using an enterprise approach to take out the rival gangs, rampant gang activity in neighborhoods on the West Side has diminished considerably.”

Hidalgo was just a child the first time he was introduced to dealing drugs. Growing up in a dysfunctional home in Buffalo, he and his siblings found ways to survive and make money on the streets while skipping school and evading foster care.

From selling his first bag of marijuana at age 10 to trafficking illegal narcotics in his late 20s, Hidalgo eventually formed “Cheko’s Crew” while recruiting friends and family to deal drugs in his lower West Side neighborhood. Having proven himself as a formidable crime boss, Hidalgo



The 7th Street Gang once operated on the lower West Side of Buffalo, New York, but gang activity in the area has diminished considerably thanks to the FBI’s Safe Streets Task Force.

joined forces with the 7th Street Gang in 2000 over mutual ties and rivalries with competing drug dealers in the community.

Hidalgo’s 7th Street Gang became a focus for the FBI’s Safe Streets Task Force, which included Bureau agents and officers from the Buffalo and New York State Police Departments. The partnership began to aggressively root out criminals after a wave of violence hit Buffalo’s lower West Side in the summer of 2009, when Hidalgo and his gang were involved in a series of murders, attempted murders, and drive-by shootings in a deadly feud with the rival 10th Street Gang.

After a series of coordinated raids by the FBI-led task force in 2009 and 2010, criminals from the 7th Street Gang and the 10th Street Gang were all brought to justice. Both gangs were successfully dismantled as a result of the Racketeering Influenced Corrupt Organizations (RICO) Act, which allows prosecutors to charge numerous associates of an enterprise with multiple crimes at the same time. In this case, the

gang members were not only found guilty of murder but of narcotics trafficking, robbery, and firearms offenses as well.

Following the FBI raids, Hidalgo managed to evade arrest but was finally captured in 2011 while trying to flee the country. He was sentenced on August 17, 2016 to 27 years in prison for his role in four murders and seven attempted murders. Like his fellow gang members, he was also convicted under the RICO conspiracy and for discharging a firearm in furtherance of a violent crime.

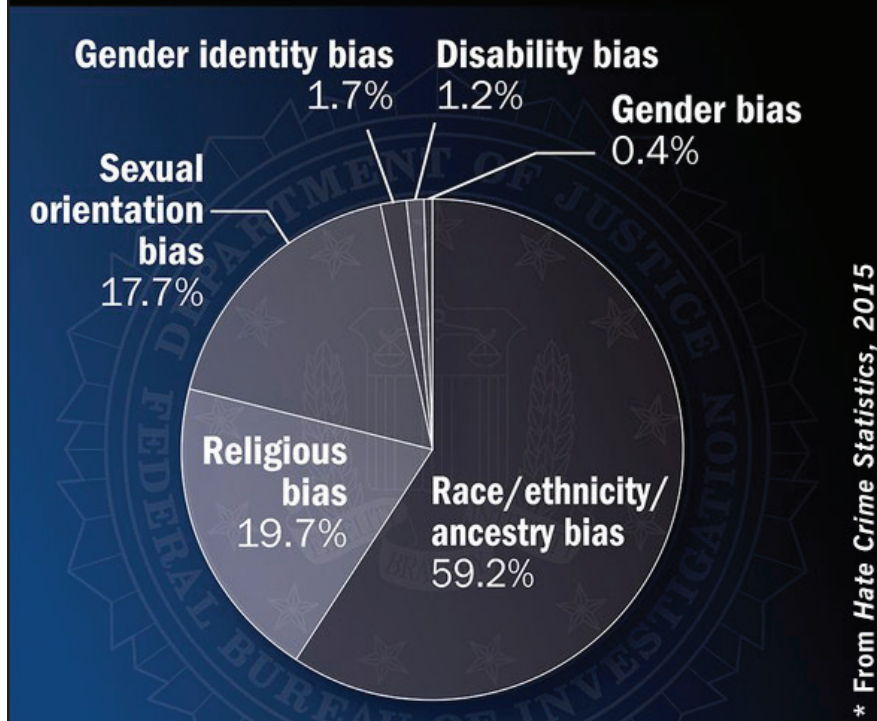
“Using an enterprise approach to take out the rival gangs, rampant gang activity in neighborhoods on the West Side has diminished considerably,” said Adam S. Cohen, special agent in charge of the FBI’s Buffalo Field Office. “The people living there feel safe in their homes, and now enjoy the quiet, once-familiar neighborhoods that decades ago built Buffalo’s historic West Side.”

Latest Hate Crime Statistics Released

Annual Report Sheds Light on Serious Issue

Hate in 2015

Here's a breakdown, by category, of why the 7,121 victims of the 5,818 single-bias incidents were targeted:



Earlier this year, a Florida man pled guilty to threatening to firebomb two mosques. A Virginia man was charged with assaulting a gay victim. And an Iowa man was convicted of stomping on and kicking the head of an African-American victim.

Hate crimes like these can have a devastating impact upon the communities where they occur, which is one of the reasons why the investigation of hate crimes that fall under federal jurisdiction is the number one priority under the FBI's civil rights program.

But in addition to its investigative work, the FBI gathers and publishes—through its Uniform Crime Reporting Program—hate crime statistics from law enforcement agencies across the country to help provide an accurate

accounting of the problem, by state and nationally. And today, the Bureau released its latest *Hate Crime Statistics* report—this one containing data for 2015—that includes information detailing the offenses, victims, offenders, and locations of hate crimes. The 2015 collection marks the 25th anniversary of the Bureau's work to compile data about bias-motivated crimes, which began in 1990.

This year's report, which contains data from 14,997 law enforcement agencies, reveals 5,850 criminal incidents and 6,885 related offenses that were motivated by bias against race, ethnicity, ancestry, religion, sexual orientation, disability, gender, and gender identity.

Additional findings in *Hate Crime Statistics, 2015* include the following:

- There were 5,818 single-bias incidents involving 7,121 victims. Of those victims, 59.2 percent were targeted because of a race/ethnicity/ancestry bias; 19.7 percent because of a religious bias; 17.7 percent because of a sexual orientation bias; 1.7 percent because of a gender identity bias; 1.2 percent because of a disability bias; and 0.4 percent because of a gender bias.
- There were an additional 32 multiple-bias incidents that involved another 52 victims.
- Of the 4,482 hate crime offenses classified as crimes against persons, intimidation accounted for 41.3 percent of those offenses, while 37.8 percent involved simple assault and 19.7 percent involved aggravated assault.
- There were 2,338 hate crime offenses classified as crimes against property, and the majority of those (72.6 percent) were acts of destruction/damage/vandalism.
- During 2015, most reported hate crime incidents (31.5 percent) happened in or near residences or homes.
- Of the 5,493 known offenders, 48.4 percent were white, 24.3 percent were black or African-American, and race was unknown for 16.2 percent of the offenders. The rest were of various other races

New to the 2015 *Hate Crime Statistics* report is the inclusion of seven additional religious anti-bias categories (anti-Buddhist, anti-Eastern Orthodox, anti-Hindu, anti-Jehovah's Witness, anti-Mormon, anti-other Christian, and anti-Sikh), as well as an anti-Arab bias motivation.

Con Artist Brought to Justice

Arizona Woman Faked Cancer, Scammed Veterans

An Arizona con artist will be spending the next 25 years behind bars after being convicted of 18 felonies in two separate trials related to her faking cancer and brazenly scamming veterans' charities out of thousands of dollars.

Chalice Zeitner's crimes were so outrageous, said FBI Special Agent Heather Rivera, "it's unlike anything I have ever seen before."

Zeitner, who skipped town and changed her name when she thought the heat was on, forged medical documents, stole identities, duped her boyfriend and physicians, and fabricated careers that included being a race car driver and a wealthy attorney who owned a law firm in South Africa. Along the way, she left a wake of victims.

Rivera, who investigated the case with Special Agent Suzanne Allen from the FBI's Phoenix Division, noted that Zeitner seemed to make a career of lies and deception. "Sadly, her path in life was all about defrauding people who trusted her."

In 2010, Zeitner told her boyfriend she had cancer and was pregnant. Zeitner said she needed to terminate the pregnancy to receive life-saving surgery in Boston. "She told her boyfriend that if she didn't terminate the pregnancy, she was going to die," Rivera said. "In reality, she did not have cancer. She was pregnant, but it was not her boyfriend's child."

Zeitner then fraudulently created documents from a Boston doctor stating she needed the life-saving surgery by a certain date. She took that document to her Phoenix OB-GYN, who petitioned the hospital to perform a state-funded,

late-term abortion so his patient's life-saving surgery could take place in Boston.

Her OB-GYN "had no reason to think she was lying," Rivera said, "because who lies about having cancer?"

Shortly after the pregnancy termination, Zeitner's boyfriend received a social media message supposedly from a family friend named Trinity stating that Zeitner was too proud to ask for help but she wanted to undergo a new type of cancer treatment in Mexico that was expensive. Trinity convinced the boyfriend to fundraise online for the treatment, and he did, raising more than \$3,000.

Trinity, it turned out, was "a fake person Zeitner created to lend legitimacy to the scheme," Allen said. Eventually, the boyfriend became suspicious when he was unable to meet Trinity in person, and doctors ultimately learned the truth about Zeitner through examinations during a subsequent pregnancy and cesarean delivery: She had never had cancer.

Her OB-GYN reported Zeitner to state medical authorities, and the Arizona Health Care Cost Containment System enlisted the FBI's help to investigate. By that time, however, Zeitner was long gone, having moved to California and changed her name.

In California, Zeitner befriended a man who ran a charity on behalf of veterans. He hoped to create a motor racing team to help raise money, and Zeitner invented a story to gain his trust. "She claimed to be a race car driver who had connections in the industry," said Allen. She also claimed to be a highly decorated veteran and falsified a military service record

to support her claim. On behalf of the charity, Zeitner started planning—and raising money—for a black-tie gala in Washington, D.C. surrounding Veteran's Day 2012.

"There is no evidence to back up any of Zeitner's claims regarding her racing cars or military decorations," Allen said, but Zeitner was persuasive. Although the gala never took place, before the scam unraveled Zeitner had stolen identities from the man and his family and used them to obtain credit cards to run up \$25,000 in personal charges. Another veteran's charity in Arizona was also scammed out of \$15,000.

The FBI caught up with the con artist in May 2015. She had fraudulently changed her name to Al Serkez and was living in Georgia. After her arrest and return to Arizona, she was indicted by the state on 11 counts related to the health care fraud. A few months later, a separate state indictment charged her with defrauding the veterans' charities.

Zeitner was deemed competent to stand trial. In both cases she mounted no defense but maintained her innocence. In April 2016, she was found guilty on the health care charges—among them, faking cancer to receive a government-funded, late-term abortion. In August 2016, after a separate trial, a jury convicted Zeitner on seven additional felony counts for scamming the veterans' charities. In September, an Arizona judge sentenced her to more than 25 years in prison.

"We are thankful," Allen said, "that this individual is going to be off the streets for many years and won't be able to take advantage of anyone else."

International Contract Fraud

U.S. Government Employee Steered \$2 Million in Micro-Dairy Contracts to His Son



Former State Department employee Kenneth Apple steered contracts for micro-dairies such as this one—being moved by heavy equipment in Iraq—to a company partially owned by his son.

In 2009, Kenneth Apple was a trusted U.S. Department of State employee who was supposed to be working in Iraq to help the Iraqi people rebuild their country after years of war. Instead, Apple decided to help himself and his son.

Part of a U.S.-led Provincial Reconstruction Team—consisting of military personnel, diplomats, and agricultural experts like himself—Apple had oversight of multi-million-dollar contracts for a variety of projects designed to stabilize Iraq's infrastructure and improve its economy.

Apple used his authority to illegally steer \$2 million in contracts for micro-dairies to a shell company located in Montana in which his son owned a 50 percent interest—and the company had no experience in the micro-dairy field.

"Apple had the ability to influence the awarding of contracts," said

Special Agent Jeff Pollack, one of the agents who investigated the case from the FBI's Washington Field Office. "He wanted to funnel money to his son. The opportunity was right in front of him, and he took it."

Micro-dairies are essentially small, mobile dairy farms. "They can even be used in the desert on a slab of concrete," Pollack said. "Housed inside a storage container is equipment that can process milk into cheese and yogurt. The idea was to provide food and create jobs for the Iraqis."

During the contract application process, Apple illegally passed critical and confidential U.S. government information to his son—Jonathan Apple—and his son's partner, who owned Xtreme Global Logistics Solutions (XGLS). The company, in turn, provided false information to

U.S. government officials about its experience and capabilities. After the contracts were awarded, Jonathan Apple earned approximately \$230,000 in profit, even though the dairy devices were never able to be commercially used.

In 2011, members of the FBI's International Contract Corruption Task Force (ICCTF)—whose mission is to investigate Americans and others overseas who steal or illegally steer U.S. funds flowing into Iraq and Afghanistan—were looking into fraud allegations at one of the Provincial Reconstruction Teams in Iraq when they came across the XGLS deal.

"We uncovered information that the awarding of the \$2 million micro-dairy contracts was not conducted in an appropriate manner," Pollack said.



This micro-dairy, made by Jonathan Apple's company, is housed in a storage container and includes equipment that can process milk into cheese and yogurt.

When investigators later confronted Apple's son, he lied about his role, stating that his father had no involvement in government contracting. When Kenneth Apple was questioned, he also lied and said he could not recall the owner of the company that won the micro-dairy contracts. "Kenneth Apple intentionally misled us," Pollack said.

"There was actually a company in Iraq that could have done this work, and this contract could have helped them. But it never happened because of the fraud."

Apple was indicted in December 2015 for wire fraud, conspiracy to defraud the U.S., obstruction of justice, and making false statements. In July 2016, a federal

jury in Virginia found him guilty on eight of nine charges. Evidence at trial showed that the micro-dairy units did not meet Iraqi Ministry of Health requirements, which was Apple's responsibility.

Last month, Apple was sentenced to 50 months in prison and ordered to pay approximately \$2 million in restitution and forfeit more than \$550,000. In November 2015, Apple's son pleaded guilty to his role in the scheme and cooperated with authorities, testifying against his father in court.

Special Agent Josh Lovett, also part of the investigative team—along with the Defense Criminal Investigative Service and the U.S. Army Criminal Investigation Command—noted that one of the worst aspects of the case was that the micro-dairies could have benefited the Iraqi people.

"The Iraqis were all for this," he said. "They put up a substantial amount of money to get these micro-dairy systems and to train their people to use them." But because of the fraudulent manner in which the contracts were awarded, and the company's failure to meet Iraqi Ministry of Health requirements, the dairy devices were never used.

"There was actually a company in Iraq that could have done this work," Lovett said. "And this contract could have helped them. But it never happened because of the fraud."

New Top Ten Fugitive

Help Us Catch a Murderer



A Jamaican man charged with murdering four people during a bloody gun battle in a Los Angeles suburb has been named to the FBI's Ten Most Wanted Fugitives list, and a reward of up to \$100,000 is being offered for information leading to his capture.

Marlon Jones is wanted in connection with the early-morning shootout that occurred on October 15, 2016 in a home being used as a restaurant. In addition to the murders, 10 individuals were wounded.

"It appears Jones was part of an East Coast Jamaican criminal group involved in the illegal distribution of marijuana, and his crew was in Los Angeles trying to settle a dispute with a rival Jamaican crew," said Special Agent Scott Garriola, a member of the FBI's Los Angeles Fugitives Task Force.

Because the crime happened so recently, Garriola said, "it is still very early in the investigation. We are not sure if the crews were business associates or if their dispute was over territory."

There are also unanswered questions about Jones himself, who is believed to have been born in Jamaica and has a long criminal record in which he has used multiple names and dates of

birth. "The biggest challenge right now besides finding him," Garriola explained, "is trying to figure out who he really is."

He added, "We're calling him Marlon Jones based on his criminal history in New York, but at this point it's anyone's guess what his actual birth name is. We don't believe he is a U.S. citizen."

Here is the information investigators currently have about Jones:

- He has an extensive and violent criminal record, including arrests for manslaughter, use of a deadly weapon during a burglary, and felony possession of marijuana.
- He uses multiple aliases and dates of birth. He has been charged with crimes in New Jersey under the name of Rasheen Brantley and has served time in New York state under the name of Floyd Evans. Other aliases include Anthony Howard, Anthony Winter, and variations on those names. Dates of birth include birth years ranging from 1970 to 1981.
- Jones is approximately 5 feet 10 inches tall and weighs between 160 and 170 pounds. He has brown eyes and black hair.

Because Jones operated predominantly on the East Coast, Garriola believes he has fled Los

Angeles. Besides strong ties to New York and New Jersey, the fugitive also has connections in Connecticut, Tennessee, the Virgin Islands, and Jamaica.

"Based on the nature of this crime, he will be armed and extremely dangerous," said Garriola, who has been involved in multiple Top Ten Fugitive investigations and believes the significant reward could make a difference in this case.

"Even for his associates involved in the narcotics business," Garriola said, "\$100,000 is still a lot of money." Garriola also stressed that anyone providing information can remain anonymous. "Everything is confidential," he said.

If you have information regarding Marlon Jones, please contact your local FBI office or the nearest U.S. Embassy or Consulate, or submit a tip on our website.

Jones is the 510th individual to be named to the FBI's Ten Most Wanted Fugitives list. Since its creation in 1950, 478 of the fugitives named to the list have been apprehended or located—158 of them as a result of citizen cooperation.

Note: Marlon Jones was taken into custody on December 2, 2016.

Cyber Operation Takes Down Avalanche Criminal Network

Servers Enabled Nefarious Activity Worldwide

It was a highly secure infrastructure of servers that allegedly offered cyber criminals an unfettered platform from which to conduct malware campaigns and “money mule” money laundering schemes, targeting victims in the U.S. and around the world.

But the Avalanche network, which was specifically designed to thwart detection by law enforcement, turned out to be not so impenetrable after all. And late last week, the FBI took part in a successful multi-national operation to dismantle Avalanche, alongside our law enforcement partners representing 40 countries and with the cooperation of private sector partners. The investigation involved arrests and searches in four countries, the seizing of servers, and the unprecedented effort to sinkhole more than 800,000 malicious domains associated with the network.

It’s estimated that Avalanche was responsible for as many as 500,000 malware-infected computers worldwide on a daily basis and dollar losses at least in the hundreds of millions as a result of that malware.

“Cyber criminals can victimize millions of users in a moment from anywhere in the world,” according to Scott Smith, assistant director of the FBI’s Cyber Division. “This takedown highlights the importance of collaborating with our international law enforcement partners against this evolution of organized crime in the virtual.”

The investigation into the highly sophisticated Avalanche network, initiated four years ago by German law enforcement authorities and prosecutors, uncovered numerous phishing and spam

campaigns that resulted in malware being unwittingly downloaded onto thousands of computers internationally after their users opened bad links in e-mails or downloaded malicious attachments. Once the malware was installed, online banking passwords and other sensitive information were stolen from victims’ computers and redirected through the intricate network of Avalanche servers to back-end servers controlled by the cyber criminals, who wasted no time in using this information to help themselves to other people’s money.

“Cyber criminals can victimize millions of users in a moment from anywhere in the world.”

One type of malware distributed by Avalanche was ransomware, which encrypted victims’ computer files until the victim paid a ransom to the criminal perpetrator. Other types of malware stole victims’ sensitive banking credentials, which were used to initiate fraudulent wire transfers. And in terms of the money laundering schemes, highly organized networks of money mules purchased goods with the stolen funds, enabling the cyber criminals to launder the illicit proceeds of their malware attacks.

How did these cyber criminals hear about the Avalanche network in the first place? Access to the network was advertised through postings—similar to advertisements—on exclusive underground online criminal forums.

Because most cyber schemes cross national borders, an international law enforcement response is absolutely critical to identifying not



just the technical infrastructure that facilitate these crimes, but also the administrators who run the networks and the cyber criminals who use these networks to carry out their crimes.

The FBI—with its domestic and international partners—will continue to target the most egregious cyber criminals and syndicates. But U.S. businesses, other organizations, and the general public need to do their part by protecting their computers and networks from malware and other insidious cyber threats. Don’t click on links embedded inside e-mails. Don’t open e-mail attachments without verifying who they’re from. Use strong passwords. Enable your pop-up blocker. Only download software from sites you trust. And make sure your anti-virus software is up to date.

Each of us securing our own devices—coupled with a coordinated law enforcement effort to combat ongoing cyber threats—will go a long way toward protecting all of us in cyberspace.

On the Waterfront

Task Force Works to Stem Flow of Illicit Drug Trafficking and Dismantle Criminal Networks

The tip came to an FBI agent regarding the drug trafficking activities of a violent Honduran street gang in New Orleans: A large shipment of cocaine ultimately bound for the U.S. was about to leave Costa Rica destined for Honduras.

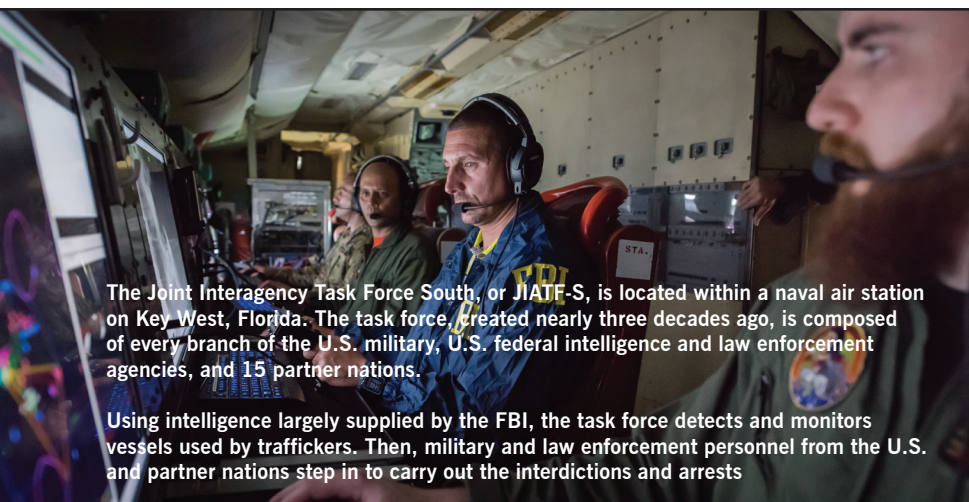
That information was relayed to FBI personnel at the Joint Interagency Task Force South (JIATF-S) in Key West, Florida, a multi-agency, international alliance whose mission is to cover 42 million square miles of territory primarily in Central and South

aircraft to locate the smugglers, who were making their way up the east coast of Nicaragua toward Honduras. Because there were no U.S. Coast Guard cutters in the vicinity to make an interdiction, the watch floor commander called the Honduran liaison officer assigned to JIATF-S and asked for assistance.

In a matter of hours, radar-equipped Honduran aircraft had taken over tracking the vessel and Honduran navy patrol boats were under way. As the navy interceptors closed in, the four

the U.S. military, U.S. federal intelligence and law enforcement agencies, and 15 partner nations whose liaison officers work side by side—has proven to be remarkably successful in the fight against the illegal drug trade.

“If you take the average price of a kilo of cocaine on Main Street USA,” said Coast Guard Rear Adm. Christopher Tomney, JIATF-S director, “we have taken more than \$6 billion worth of illicit profits out of the system. We’re talking hundreds of tons of cocaine that have been intercepted.”



The Joint Interagency Task Force South, or JIATF-S, is located within a naval air station on Key West, Florida. The task force, created nearly three decades ago, is composed of every branch of the U.S. military, U.S. federal intelligence and law enforcement agencies, and 15 partner nations.

Using intelligence largely supplied by the FBI, the task force detects and monitors vessels used by traffickers. Then, military and law enforcement personnel from the U.S. and partner nations step in to carry out the interdictions and arrests



America to stem the flow of illegal drugs and to disrupt and dismantle sophisticated narco-trafficking networks. Much of that work is carried out on the high seas.

The Honduran traffickers had set out from Limón, Costa Rica. Their “go-fast” boat—a small, low-profile vessel favored by smugglers—was packed with 300 kilos of cocaine and a cache of military-grade weapons, including M16 rifles and grenade launchers.

When intelligence sources confirmed that the boat was in the water, officers on the watch floor at JIATF-S requested that the U.S. Navy launch a P3 surveillance

smugglers beached their craft and ran into the jungle, firing on their pursuers as they fled. In the end, the criminals were apprehended, along with the drugs and weapons. The four are currently imprisoned in Honduras.

From a single piece of intelligence provided to the FBI in New Orleans, an international response was quickly set in motion that kept a large quantity of drugs from entering the United States. At JIATF-S, scenarios like this play out nearly every day.

Since its creation nearly three decades ago, the task force—composed of every branch of

The challenges posed by narco-traffickers, however, remain enormous. “The threats we go against know no boundaries,” Tomney said. “These are threats that affect multiple agencies and multiple nations. It not only takes a whole government approach to go after these problems, it really takes a whole hemisphere approach.”

The task force succeeds by integrating intelligence gathering and sharing with streamlined and highly coordinated tactical operations. Partner nations significantly extend the reach of U.S. capabilities. Everyone works toward the common goal of

stopping the illicit drug trade. As one task force member noted, “We all take the field as one team.”

Using intelligence largely supplied by the FBI, the task force detects and monitors the go-fast boats and difficult-to-detect semi-submersible vessels used by traffickers. Then, military and law enforcement personnel from the U.S. and partner nations step in to carry out the interdictions and arrests.

“It starts with narcotics, but the criminal networks are also smuggling weapons, bulk currency, trafficking humans, and using

said Chianella, who was recently appointed a JIATF-S vice director.

Partner nations send their best and brightest officers to work at the task force for one- and two-year assignments, and when they return to their home countries—often to assume leadership positions in their organizations—they have built lasting relationships with their fellow liaison officers and U.S. contacts.

Lt. Col. Gustavo Alvarez, a Honduran Army officer, had just arrived in Florida as the JIATF-S

Cmdr. Jose Jose-Vasquez, a JIATF-S liaison officer from the Dominican Republic Navy, agreed. “If I have to make a contact with the Colombian liaison, for example, I just have to look in the office. I don’t need a passport or a visa or a diplomatic procedure. In a matter of minutes, we have the information needed to be successful.”

Where drug traffickers are concerned, minutes can make a difference. On the JIATF-S watch floor any time of day or night, targeting officers and intelligence



sophisticated money laundering techniques,” said FBI Unit Chief Brett Chianella, who heads the Bureau’s staff at JIATF-S. “Those networks are organized, armed, and well-financed, and they have ties to corrupt public officials and even foreign terrorist fighters,” he added. “The drugs are one spoke in the wheel of all this organized crime activity.”

One of the task force’s priorities is to stop the flow of drugs at their source of supply rather than after the contraband enters the U.S. and is distributed. “Either you deal with it 1,500 miles away or you deal with it after it crosses our borders,”

liaison officer in March 2015 when he assisted with the FBI case out of New Orleans. He saw firsthand how the task force model of integrating intelligence and operations gets results.

“One of the biggest takeaways when you come here,” he said, “is that the foreign liaison officers are all just a few steps away, one office to the other.” That means information flows into the task force, Alvarez said, “but it also starts going between the other countries of interest. So the information flow really grows exponentially.”

analysts may be tracking dozens of vessels on the vast Pacific Ocean or Caribbean Sea suspected of carrying cocaine and other contraband. They must decide how to deploy limited military resources to track these vessels and to target them for interdictions.

Self-propelled semi-submersible craft (SPSS) are the most highly prized catches because they carry the most drugs, anywhere from eight to 10 metric tons of cocaine—that’s roughly \$300 million in street value. But these vessels are designed for stealth, with very little of the craft showing above the water line.

"It's very difficult to find them on radar, said Gerry Canavan, a retired Coast Guard officer who joined the FBI as an analyst helping to target vessels suspected of carrying drugs. "If it's not flat and calm, the radar probably isn't going to pick up an SPSS," he said. The task force has other technical means at its disposal, but intelligence gained through human and other sources is critical to the process.

"The FBI doesn't have planes or ships at JIATF-S," said Kevin Lopez, also a former Coast Guard officer who joined the FBI to work on the task force. "The Bureau provides information that will help the task force position its aircraft

and ships to locate that go-fast or SPSS."

As successful as JIATF-S has been, Chianella and others estimate that the drugs interdicted annually represent only about 20 percent of the total amount being smuggled into the U.S. "As long as there's a demand for cocaine or any illicit contraband in the United States," he said, "the cartels and criminal networks will find a way to move their product."

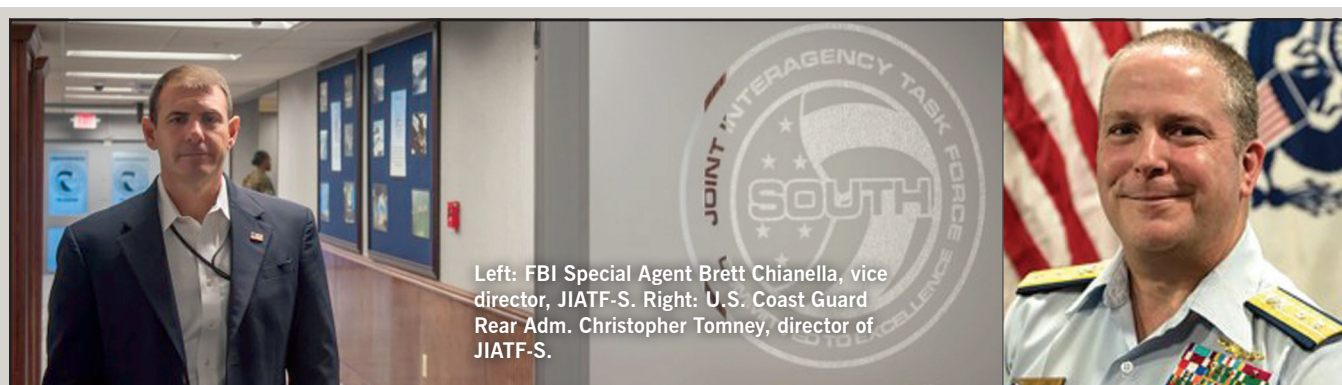
The drug trade, added the Dominican Republic's Jose-Vasquez, "is like an energy—you cannot destroy it; it only transforms in another manner. This problem is a reality that we have and that

we have to work against," he said. "Working together makes us stronger. Being in this organization provides us with better tools to work against these common threats."

"We are fighting a transnational threat," JIATF-S Director Tomney explained. "No one nation, including the United States, has all the tools, all the capabilities, and all the resources to go it alone. By working together," he said, "we can bring stability to the region and keep more than drugs in check."



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/jiatfs.



'A Seat at the Table'

In December 2015, Special Agent Brett Chianella, who leads the FBI's team at JIATF-S, was appointed vice director of the task force—the first FBI fully integrated Department of Defense position. Chianella's new role is meant to further leverage the Bureau's intelligence gathering abilities and to acknowledge the important role the FBI plays in the continuing success of the task force.

The position underscores how unified the FBI is with the Department of Defense in carrying out the task force's mission—to

monitor and detect the most violent illicit traffickers in the Western Hemisphere and to disrupt and dismantle transnational criminal organizations.

"This has been a win-win proposition," said Rear Adm. Christopher Tomney, JIATF-S director. "The FBI vice director provides key insights and experiences that I just don't have as a senior Coast Guard officer. Nowhere in the command group, because we are such a melting pot of organizations, do we have that senior Department of Justice investigatory experience." The

vice director position, he added, will be "completely woven into the command structure of this organization."

"The FBI and the military share the same philosophy on combating transnational criminal networks and organized crime," Chianella said. "To have the FBI fully integrated within the Department of Defense to disturb and dismantle violent networks supports a whole of government approach and takes the fight to them, before it affects us at home."



By the Numbers

The Joint Interagency Task Force South (JIATF-S) was created in 1989 to monitor and detect narco-trafficking and to disrupt and dismantle the criminal organizations that profit from the illicit drug trade. The Department of Defense-funded operation, which falls under the military's U.S. Southern Command, has responsibility for 42 million square miles of territory in the Western Hemisphere.

- JIATF-S is composed of every branch of the U.S. military, U.S. federal intelligence and law enforcement agencies such as the FBI and the Drug Enforcement

Administration, and 15 partner nations whose liaison officers work side by side at the task force headquarters in Key West, Florida. Five additional countries are in the process of joining the task force.

- Since its creation, JIATF-S has intercepted hundreds of tons of cocaine worth an estimated street value of \$6 billion. It is estimated that the task force has been responsible for half of all the cocaine interdicted in the world.
- Within the last three years, nearly 700 non-U.S. persons were indicted and brought to the U.S. to face criminal charges as a result of task force operations.

Some 150 criminal networks were identified during that same period, and 60 of those networks were dismantled.

- In 2015, JIATF-S operations led to the interdiction of seven self-propelled, semi-submersible (SPSS) vessels. Designed specifically for smuggling, these craft carry anywhere from eight to 10 metric tons of cocaine with a street value of \$300 million. The FBI provided intelligence and investigative resources in six of those seven cases.
- For more information about JIATF-S: <http://www.jiatfs.southcom.mil/>

2015 NIBRS Crime Data Released

Report Contains More Detail on Criminal Offenses

Today, the FBI released details on more than 5.6 million criminal offenses reported by law enforcement to the National Incident-Based Reporting System (NIBRS) in 2015. This latest Uniform Crime Reporting (UCR) Program's report, *National Incident-Based Reporting System 2015*, offers a wide range of information about victims, known offenders, and relationships between the two for 23 categories comprised of 49 offenses.

The NIBRS is slated to replace the traditional Summary Reporting System by January 1, 2021, establishing it as the national standard for crime reporting. The move is backed by a host of criminal justice leaders, including the Criminal Justice Information Services Division's Advisory Board Policy Board (a multi-agency group), the International Association of Chiefs of Police, the Major Cities Chiefs Association, the Major County Sheriffs' Association, and the National Sheriffs' Association.

Why NIBRS? When used to its full potential, the system will identify with precision when and where crime takes place, what form it takes, and the characteristics of victims and perpetrators. Armed with that information, law enforcement can better identify the resources it needs have the ability to use those resources more efficiently and effectively.

This latest NIBRS report includes a message from FBI Director James Comey about the importance of the new reporting system and of the National Use of Force Data Collection. He said, "We need more transparency and accountability in law enforcement. We also need better, more informed



conversations about crime and policing in this country. To get there, we are improving the way this nation collects, analyzes, and uses crime statistics and data about law enforcement's use of force."

Director Comey also expressed his appreciation to law enforcement agencies around the country who submitted NIBRS data during 2015. "By providing this data," he said, "they are playing a critical role in helping us to better understand what is happening in our nation."

"We need more transparency and accountability in law enforcement. We also need better, more informed conversations about crime and policing in this country."

Participation via NIBRS did increase during 2015 by 128 agencies, for a total of 6,648 agencies representing coverage of more than 96 million people. But while the number of agencies participating in NIBRS increases each year, the 2015 coverage representing just 36.1 percent of all law enforcement agencies that participate in the UCR Program shows that there is still some work to be done.

The FBI continues working to expand NIBRS participation. Most recently:

- Fifty-six agencies began reporting NIBRS data;
- Funding was awarded to seven

state programs and 17 agencies through the FBI and the Bureau of Justice Statistics' Joint Crime Statistics Exchange initiative;

- The Department of Defense was certified as NIBRS compliant, making DOD the first federal agency to transition to NIBRS; and
- The NIBRS Modernization Study began, assessing whether improvements to NIBRS are needed.

Here are some highlights from the new NIBRS report:

- NIBRS agencies reported 4,902,177 incidents that involved 5,668,103 offenses, 5,979,330 victims, and 4,607,928 known offenders.
- Of the report offenses, 62.9 percent involved crimes against property, 23.2 percent involves crimes against persons, and 14 percent included crimes against society (like gambling and prostitution).
- Of the 4,158,264 individual victims, 23.8 percent were between 21 and 30 years of age; a little more than half (50.9 percent) were female; and the majority of victims (72.0 percent) were white, while the next largest percent (20.8) were black or African-American.
- Of the known offenders, more than 44 percent were between the ages of 16 and 30, and most offenders (63.3 percent) were male.

More details on the data in NIBRS 2015 can be found on our interactive NIBRS map and the agency-level offense tables, which present statistics for each that reported 12 months of NIBRS data in 2015.

International Cyber Sweep Nets DDoS Attackers

California Grad Student Arrested in Operation Aimed at Young Hackers

A 26-year-old student in California was among nearly three dozen suspects arrested last week in a cyber crime sweep involving 13 countries.

Sean Sharma, a graduate student at the University of Southern California, was arrested December 9, 2016 and charged with cyber crimes for his role in a distributed denial of service (DDoS) attack that knocked a San Francisco chat service company's website offline. DDoS attacks flood websites and their servers with massive amounts of data, leaving them inaccessible to users. Sharma purchased a tool to mount his cyber attack, according to the charges against him.

The arrest occurred during an operation aimed at users of "DDoS for hire" services, which can be used to target computers and websites of their choosing. Over five days beginning on December 5, law enforcement agencies conducted 101 interviews and arrested 34 suspects in the sweep, which was coordinated from The Hague in the Netherlands by Europol's European Cyber Crime Centre (EC3). Europol, the law enforcement agency of the European Union, assisted participating countries in their efforts to identify suspects—many under the age of 20—by sharing intelligence and analytical support. Actions within the United States were coordinated by the International Cyber Crime Coordination Cell, or IC4, hosted by the FBI in the Washington, D.C. area.

The case against Sharma is being investigated by the FBI San Francisco Field Office's San Jose Resident Agency. If convicted, Sharma could face up to 10 years

in prison. In a statement released today, the FBI said the nature of cyber crimes often requires a coordinated response, since subjects could be operating from anywhere in the world.

"No law enforcement agency or country can defeat cyber crime alone."

The operation marked the kick-off of a prevention campaign to raise awareness of the risks of young adults being lured into committing cyber crimes. In a press release about the operation, Europol said teenagers who become involved in cyber crimes often have skill sets that could be put to positive use through a career in computer programming or cyber security.

"DDoS tools are among the many specialized cyber crime services available for hire that may be used by professional criminals and novices alike," said Steve Kelly, FBI unit chief of IC4. "While the FBI is working with our international partners to apprehend and prosecute sophisticated cyber criminals, we also want to deter the young from starting down this path."

Europol identified examples of cyber crimes that involve predominantly young offenders. They include:

- Hacking, or gaining access into someone's computer network without their permission, and then taking control and/or taking information from other people's computers.
- Making, supplying, or obtaining malware (malicious software), viruses, spyware, botnets, and remote access Trojans.

- Carrying out a DDoS attack or "booting" a DDoS—booting someone offline, for example, while they are playing online games.

"Today's generation is closer to technology than ever before, with the potential of exacerbating the threat of cyber crime," said Steve Wilson, head of the EC3. "Many IT enthusiasts get involved in seemingly low-level fringe cyber crime activities from a young age, unaware of the consequences that such crimes carry."

Last week's law enforcement actions took place in Australia, Belgium, France, Hungary, Lithuania, the Netherlands, Norway, Portugal, Romania, Spain, Sweden, the United Kingdom, and the U.S.

The arrest of Sharma in La Canada, California, was just one of the investigative activities conducted last week by cyber task forces in the U.S. The efforts included interviews that did not result in arrests but highlighted the seriousness of engaging in cyber crimes, which is a top priority of the FBI. In a statement released today, the FBI said the nature of cyber crimes often requires a coordinated response, since subjects could be operating from anywhere in the world.

"No law enforcement agency or country can defeat cyber crime alone, the Bureau statement said. "This demands a collective global approach."

New Top Ten Fugitive

Help Us Capture a Murderer

FBI TEN MOST WANTED FUGITIVE
UNLAWFUL FLIGHT TO AVOID PROSECUTION - MURDER
ROBERT FRANCIS VAN WISSE


Age-progressed photograph

Aliases: Francisco Salas, Roberto Francisco Salas, Robert F. Vanwisse, Robert Wisse, Robert F. Van Wisse, Robert Francis Vanwise, Robert Vanwise

A Texas man charged with the strangulation murder of a 22-year-old woman in 1983 has been named to the FBI's Ten Most Wanted Fugitives list, and a reward of up to \$100,000 is being offered for information leading to his capture.

Robert Francis Van Wisse, a 19-year-old college student at the time of the murder, is now 51 years old and has been on the run for more than two decades. "No matter how much time has passed," said Special Agent Justin Noble, a member of the FBI's Central Texas Violent Crimes Task Force in Austin who is investigating the case, "it's important that we finally get justice for the victim and her family."

The victim, married with a 1-year-old daughter, worked as a janitor at the University of Texas at Austin. On the September night of the murder, Van Wisse was in the building late registering for a course.

The victim's body was found in a restroom the next morning. An autopsy revealed that she had been sexually assaulted and strangled with a wire. Investigators

determined that Van Wisse was the last person seen in the building before the murder. "He was initially ruled out as a suspect," Noble explained, "because DNA and other tests were not as sophisticated then as they are today."

The case went cold for a decade, until the early 1990s, when an Austin Police Department detective submitted crime scene evidence for new DNA tests—tests that took advantage of the latest technology. "The results pointed directly to Van Wisse," Noble said.

When Van Wisse learned that he was being evaluated again as a suspect, he fled. In 1996, Texas charged the fugitive with capital murder, and the following year he was charged federally with unlawful flight to avoid prosecution.

"He was a college student whose parents were both professionals," Noble said. "He grew up going to the best schools and living in the nicest neighborhood. He had the future in front of him," Noble added, "and yet it appears he murdered a young woman making minimum wage trying to support her family and young child."

When Noble read the original arrest affidavit, he believed the killer had acted impulsively. "But after studying the crime scene reports and autopsy," he said, "the evidence clearly suggests that this was a premeditated act."

Noble noted that Van Wisse's family owns multiple properties in Mexico and in Guatemala. "He's a smart guy and he's bilingual," Noble said of the fugitive. "He could be anywhere."

At a press conference held today at the federal courthouse in Austin, authorities said the publicity effort to capture Van Wisse will include a social media advertising campaign targeted to specific locations in the U.S. and abroad. "We have also identified more than 30 individuals who have had close ties to Van Wisse," Noble said, "and we are going to be in contact with all of them. Somebody knows something, and \$100,000 is a lot of money." Noble stressed that anyone providing information to the FBI can remain anonymous.

"We need to catch this guy," he said. "The victim and her family deserve nothing less. It doesn't matter that the murder took place more than three decades ago—to the victim's family, it was like it was yesterday."

If you have information regarding Van Wisse, contact your local FBI office or the nearest U.S. Embassy or Consulate, or submit a tip on our website.

Note: Robert Francis Van Wisse was taken into custody on January 26, 2017.

New Top Ten Fugitive

Help Us Catch a Killer

A Wisconsin man wanted for a double homicide is the newest addition to the FBI's Ten Most Wanted Fugitives list, and a reward of up to \$100,000 is being offered for information leading to his capture.

Terry A.D. Strickland, a 24-year-old Milwaukee resident, is charged with fatally shooting two men last July during a fight outside the house where he rented a room. After the murders, he fled the scene, abandoning his 18-month-old daughter.

"We don't know all the details surrounding the shooting and what prompted it," said Special Agent Chad Piontek, who is investigating the case from the FBI's Milwaukee Division, "but we know that Strickland is extremely dangerous and he is a threat to the community."

Milwaukee Police Department officers responded to multiple reports of a shooting on the afternoon of July 17, 2016. The bodies of two men—ages 38 and 39—were found outside the residence where Strickland appeared to be living with his daughter.

According to witnesses, a group of approximately seven or eight men were in front of the residence arguing. Strickland entered the house and allegedly returned with a .40-caliber handgun and began shooting into the group. One man who attempted to stop the argument ended up on the ground, and Strickland reportedly stood over the unarmed victim and shot him repeatedly before turning and shooting another unarmed victim in the head. After the shooting, Strickland fled, leaving his daughter behind in the residence.

FBI TEN MOST WANTED FUGITIVE

UNLAWFUL FLIGHT TO AVOID PROSECUTION - TWO COUNTS OF FIRST DEGREE INTENTIONAL HOMICIDE (USE OF A DANGEROUS WEAPON)

TERRY A.D. STRICKLAND



Photograph taken in 2016



CAPTURED

Aliases: Teery A. Strickland, Terry A. Strickland, Terry Antonio Strickland

Strickland is 6 feet 2 inches tall, weighs approximately 240 pounds, and has black hair and brown eyes. He has no known scars or tattoos. The fugitive has ties to Wisconsin, Illinois, and Indiana and is not known to have traveled outside the United States.

"We are asking for the public's assistance to help us locate and apprehend Strickland before he hurts anyone else. There is no question that he is a danger to the community."

"The most recent information we have is that he might be in a Chicago suburb," Piontek said, noting that the murder weapon was not recovered and it is likely that Strickland is armed.

Strickland is the 512th person to be placed on the FBI's Ten Most Wanted Fugitives list, which was established in 1950. Since then, 479 fugitives have been apprehended or located—and 159 of them were captured or located as a result of

citizen cooperation.

"We are asking for the public's assistance to help us locate and apprehend Strickland before he hurts anyone else," Piontek said. "There is no question that he is a danger to the community. The fact that he abandoned his daughter while fleeing says a lot about his character."

If you have information regarding Strickland, contact your local FBI office or the nearest U.S. Embassy or Consulate, or submit a tip on our website. Individuals should take no action themselves, Piontek said, adding that any information provided to the FBI can remain confidential.

"We are confident that the \$100,000 reward will provide a great deal of incentive to someone with information about Strickland's whereabouts," Piontek said. "Even his friends and family should be frightened about the violence he is capable of."

Note: Terry A.D. Strickland was taken into custody on January 15, 2017.

Protecting Vital Assets

Pilfering of Corn Seeds Illustrates Intellectual Property Theft



A Chinese national sentenced last month in Iowa for stealing trade secrets wasn't looting blueprints for military weapons, computer software, or high-tech electronics. Mo Hailong's efforts were considerably more grounded—he was stealing corn.

The object of Mo's five-year conspiracy was to steal proprietary corn seeds from fields in Iowa—and across the farm belt of the Midwest—and send them to China, where Mo's employer, a Chinese corn seed company, was based. Contained within the stolen inbred seeds—which, unlike common hybrid seeds, can be replanted year after year—were the valuable trade secrets of U.S. companies DuPont Pioneer and Monsanto.

Mo, 46, a legal permanent resident of the U.S. with a home in Florida, was sentenced on October 5, 2016 to three years in prison and ordered to forfeit two farms in Iowa and Illinois that were purchased to support and provide cover for his criminal activities. The case, which led agents on cat-and-mouse

surveillance operations across the Midwest and took them on a deep dive into the biotechnology of proprietary corn breeding, came to light following a routine liaison visit in 2012 by FBI agents to DuPont Pioneer's offices near Des Moines.

"At the end of that meeting, they brought up an incident where an Asian male had been digging in one of their grower fields," said Special Agent Mark Betten, who at the time worked in the FBI Omaha Division's Des Moines office. Grower fields operate like laboratories where companies can test their products. The fields are often in remote locales, Betten said, so when a field manager spotted Mo digging there on May 3, 2011, he became suspicious and confronted him. Mo told the field manager he worked for a local university, then hurriedly drove away as the field manager noted his license plate number. By the end of the liaison meeting, the FBI agents had Mo's name and address in Boca Raton.

Soon after, on a separate visit to another Des Moines-area seed producer, company officials said that they had recently been to China on a business trip and shared with whom they had met. Among the names was Mo Hailong's. To Betten, it seemed like more than just a coincidence. When the agent showed a picture of the Florida man who had been caught digging in the Iowa field, company officials said it was the same guy they had met in China.

"Our counterintelligence mission is to protect America's vital assets. It just so happens that in this case, the vital assets are corn seeds, which take a tremendous amount of time and money to develop."

"That's kind of how the case got started," Betten said. "I was full-time on it from that point on."



The case would expand to include five other conspirators and required tracking their disparate whereabouts across six states and thousands of miles. “Surveillance is very difficult in rural areas, out in cornfields,” Betten said. “The logistics were a challenge.”

Another challenge was fully understanding and then laying out crucial elements of the complicated case to judges and courts to obtain necessary warrants. “When you’re writing affidavits explaining what the intellectual property is and how they’re stealing it—while protecting each company’s property right—that was all scientifically very challenging to articulate,” Betten said.

The investigation revealed that Mo and his co-conspirators were gathering seeds from farms across the Midwest and packaging them to send in bulk to China. In one example, in May 2012, Mo and two others tried to ship 250 pounds of corn seeds from Illinois to Hong Kong, according to the indictment.

Mo was arrested on December 12, 2013 and indicted, with five others, on charges of plotting to steal seeds. According to the criminal complaint, Pioneer DuPont executives estimated the theft of this type of seed would result in the company losing five to eight years of research and at least \$30 million.

Bill Priestap, assistant director of the FBI’s Counterintelligence Division, said corn seeds developed in the U.S. are no different than other types of intellectual property when it comes to being targets for theft or espionage.

“If a company in the U.S. is a world leader in something, it’s likely being targeted,” Priestap said, adding that an essential piece of the Bureau’s counterintelligence strategy is to raise awareness of that threat.

“People may think that it’s just a couple of farms in Iowa. But it’s about more than that,” he said. “Our counterintelligence mission is to protect America’s vital assets. It just so happens that in this case, the vital assets are corn seeds,

which take a tremendous amount of time and money to develop.”

A similar case in Kansas further illustrates Priestap’s point. On December 12, 2013—the same day Mo was arrested in Iowa—two agricultural scientists from China were arrested and charged with trying to steal samples of rice seeds from an Arkansas research facility. One pleaded guilty in the case last month and the other is awaiting trial.

Betten said it was by design that the arrests in the corn and rice cases occurred at the same time. “We didn’t want to spook the others,” he said. “We were afraid if Omaha acted before Kansas City that their subject would catch wind of it, and vice versa.”

In the corn case, Mo pleaded guilty last January. His indicted co-conspirators are believed to be in China.

Corruption on the Border

New Campaign Enlists the Public's Help



The border awareness campaign includes publicity outreach efforts, such as the poster above, in 10 FBI field offices whose areas of responsibility include border crossings, airports, and seaports.

During his trial on public corruption charges in 2013, former U.S. Customs and Border Protection officer Hector Rodriguez admitted that he had been receiving bribes of cash and luxury items for two years in return for admitting illegal aliens into the U.S. through his inspection lane at the San Ysidro Port of Entry in San Diego, California.

While the overwhelming majority of law enforcement officers and public officials who work at the country's ports and borders are honest and dedicated, even one corrupt official like Rodriguez can pose a serious threat to the nation's security—because what if one of those individuals smuggled through a port of entry is a terrorist carrying a bomb?

For that reason, the FBI—in collaboration with the Department of Homeland Security—is launching a campaign to raise awareness about the dangers of border corruption so that citizens and government employees who see

corruption or suspicious activity will call the FBI to report it.

“The point of our public awareness campaign is that we need your eyes and ears to help keep the country safe.”

“Public corruption is the FBI’s top criminal priority,” said Sergio Galvan, chief of the Bureau’s Public Corruption Unit at FBI Headquarters in Washington, D.C. “It is critical for us to engage the public to help stop these crimes. We’re not expecting citizens to be detectives,” Galvan explained, “but if you see something that doesn’t seem right, report it. If you notice someone going through security without being searched, or if you work on the border and know someone in your agency that is looking the other way, call the FBI.”

The border awareness campaign will include publicity outreach efforts in 10 FBI field offices whose

areas of responsibility include U.S. ports of entry such as border crossings, airports, and seaports. The cities are Buffalo, New York; Detroit, Michigan; El Paso and San Antonio, Texas; Fargo, North Dakota; Los Angeles and San Diego, California; Miami, Florida; Phoenix, Arizona; and Seattle, Washington.

“We want to know what people are seeing and hearing,” Galvan said, “whether you are a frequent traveler, a truck driver, or a law enforcement official who works on the border.”

Hector Rodriguez pleaded guilty to receiving bribes and bringing aliens into the country for financial gain. In 2013 he was sentenced to five years in prison and three years of supervised release for receiving thousands of dollars in cash, along with Rolex watches and an expensive vehicle, for looking the other way. But public corruption on the border is by no means limited to the Southwest border.



Posters and banners in English and Spanish encourage the public to report suspected border corruption to the FBI at tips.fbi.gov. All posters are available to view and download.

The FBI has 22 border corruption task forces and working groups across the country staffed by 39 local, state, and federal partner agencies, including U.S. Customs and Border Protection, the Drug Enforcement Administration, and the Transportation Security Administration. More than 250 officers are working cases and gathering intelligence to stop public corruption along all U.S. ports of entry.

And while federal, state, and local officials who serve along our borders are working hard to keep the country safe from outside threats, “when even one of those individuals is compromised, it creates a grave situation,” Galvan said. “What I would like to say to the public and to individuals who work in agencies that serve at the border is that the FBI is here to help you—but we can’t help if we don’t get information. If you see something, pick up the phone. Call

your local field office or submit a tip on our website. The point of our public awareness campaign,” he added, “is that we need your eyes and ears to help keep the country safe.”



Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/reportbordercorruption.

A Look Back: A Small Office with a Big Mission

The FBI's World War II-Era Cover Company at Rockefeller Center



Employees and visitors board an elevator inside the RCA Building at Rockefeller Center (circa 1940), site of the FBI's first cover office for its covert program known as the Special Intelligence Service. (© 2015 Rockefeller Group Inc/Rockefeller Center Archives)

Everyone knows that the holiday season is well under way when the giant Christmas tree is lit at Rockefeller Center in New York City. What is less well known, however, is the connection between Rockefeller Center and the birth of America's civilian foreign intelligence efforts.

It was 1940 and the world had plunged into war the previous summer. Although America remained neutral at that time, it did not ignore the massive international threat, and an FBI operation—small but critical to America's response to that threat—was centered in the heart of New York City in Rockefeller Center. It was called the Importers and Exporters Service Company and operated out of room 4332 at 30 Rockefeller Center—the RCA

Building—beginning in August 1940.

Importers and Exporters was the Bureau's first attempt to set up a long-term cover company for our covert program, the Special Intelligence Service (SIS). The SIS was the United States' first civilian foreign intelligence service and was less than a year old. Under a 1940 agreement signed by the Army, Navy, and FBI and approved by President Roosevelt, the FBI was given responsibility for "foreign intelligence work in the Western Hemisphere." This saw us gathering intelligence about espionage, counterespionage, subversion, and sabotage concerns—especially about Nazi activities—pertaining to civilians in South America, Central America, and the Caribbean. We were to create

an undercover force that would proactively protect America's security from threats in our international neighborhood. Given that our past success was mostly in criminal matters, taking on this task would be a steep learning experience.

To begin, we wanted to center the operation away from traditional FBI facilities and wanted to anchor it in commercial efforts, because they would provide the freedom of movement and access our agents would need. Although it is not clear why the Bureau chose to establish a presence at 30 Rock, it likely had something to do with the support that Nelson Rockefeller had provided to President Roosevelt's intelligence work. Furthermore, on multiple occasions after the SIS's creation,

our personnel were afforded cover by Nelson Rockefeller's Office of the Coordinator of Inter-American Affairs.

The RCA Building placed the FBI within a hotbed of foreign activity, both allied and enemy. The Rockefellers provided space in the same building at little or no cost to British Security Coordination, an intelligence agency/liaison service. It also hosted Italian, German, and Japanese tenants until the U.S. government detained them as enemy aliens when America entered World War II. And the Soviet Union had office space in the building as well.

Of course, the sign on the door did not read "FBI/SIS—Spies Welcome." Instead, the Importers and Exporters Service Company—which never imported or exported anything—was supposed to be completely unidentifiable with the Bureau and would provide "backstopping" or cover identities, employment, and other necessary tools for our agents to operate undercover. With these new identities, representatives of the company were to travel throughout the hemisphere to collect intelligence and help to disrupt the Axis threat.

It looked good on paper; however, the plan took an unexpected turn because Bureau personnel had to fend off daily advances from unsuspecting salesmen and other parties knocking on the door wanting to do business with the new company. The FBI ended up shutting down the Importers and Exporters business in June 1941, but we kept the office itself open until November 1945, using it to quietly handle logistics for deploying SIS personnel.



Exterior of the RCA Building at Rockefeller Center during the 1940s. (© 2015 Rockefeller Group Inc/Rockefeller Center Archives)

Although the Importers and Exporters Service Company was a short-lived enterprise, its method of operation, providing what is known as "non-official cover" in the spy business, became crucial to the SIS's intelligence activities and its subsequent successes. Learning from its Importers and Exporters experience, the Bureau—instead of maintaining one single cover company—enlisted the assistance of accommodating U.S. companies that agreed to provide cover jobs for Bureau personnel. (And in a boon for some of those companies, many of the individuals who filled these positions worked so enthusiastically that they became

nearly indispensable to their cover employers.)

Room 4332 at 30 Rock and what went on there more than 70 years ago is little remembered now—the room itself doesn't even exist anymore because the floor it was located on has an open plan today. However, those who enjoy the Christmas tree and skating rink at Rockefeller Center during the holiday season might take a minute to reflect on the building's role in America's first civilian foreign intelligence service.

Index

ART THEFT

A Wartime Loss Found: FBI Assists Polish Government in Recovering Painting Lost During WWII, pages 23-24

Darwin Letter Recovered: FBI Returns 1875 Correspondence to Smithsonian Archives, page 58

CIVIL RIGHTS

Human Rights: FBI Reaching Out About Female Genital Mutilation, page 51

Civil Rights and Law Enforcement: Director Speaks at Birmingham Conference, pages 56-57

Human Trafficking: Guatemalan Migrants Exploited in Forced Labor Scheme, page 95

Report from Thailand, Part 1: Confronting the Child Sex Trade in Southeast Asia, pages 96-97

Report from Thailand, Part 2: A New Emphasis on Helping Child Victims, pages 98-99

Report from Thailand, Part 3: It Takes a Village, pages 100-101

Report from Thailand, Part 4: Strengthening Investigations Through Collaboration, pages 102-103

Latest Hate Crime Statistics Released: Annual Report Sheds Light on Serious Issue, page 122

COUNTERTERRORISM

Countering Violent Extremism: FBI Launches New Awareness Program for Teens, pages 14-15

FBI Tip Line: Web Portal, Created in 2001, Receives 'Actionable' Tips Daily, page 22

Man Gets 16 Years for Attempting to Purchase Ricin: Use of Stolen Identity Adds to Length of Sentence, page 40

Countering Terrorism: Inside the Mufid Elfgeeh Investigation, page 52

Animal Rights Extremists: Pair Took Law into Their Own Hands, page 60

Director Provides Update on Orlando Shootings Investigations, page 61

Identifying the Vulnerabilities: Weapons of Mass Destruction Directorate Marks 10 Years, pages 76-77

Remembering 9/11: FBI Has Evolved in Response to Changing Threats, page 94

CRIMES AGAINST CHILDREN

Child Sexual Exploitation: Threat from Pedophiles Online is 'Vast and Extensive', page 50

Help Us Find Them: National Missing Children's Day 2016, page 54

Child Sex Tourism: Alaska Man Receives Prison Term for Crimes Committed in Cambodia, page 55

'A Predator in Every Sense of the Word': Subject Gets 70 Years for Theft Scheme and Producing Child Pornography, page 79

Fugitive Apprehended: Alleged Child Abuser Was on the Run for 23 Years, page 88

Report from Thailand, Part 1: Confronting the Child Sex Trade in Southeast Asia, pages 96-97

Report from Thailand, Part 2: A New Emphasis on Helping Child Victims, pages 98-99

Report from Thailand, Part 3: It Takes a Village, pages 100-101

Report from Thailand, Part 4: Strengthening Investigations Through Collaboration, pages 102-103

Operation Cross Country X: Recovering Underage Victims of Sex Trafficking and Prostitution, pages 110-111

CRIMINAL JUSTICE INFORMATION SERVICES

Tracking Animal Cruelty: FBI Collecting Data on Crimes Against Animals, page 12

Latest Crime Statistics Released: Increase in Violent Crime, Decrease in Property Crime, page 105

LEOKA Report Released: 41 Officers Feloniously Killed in 2015, page 112

Latest Hate Crime Statistics Released: Annual Report Sheds Light on Serious Issue, page 122

2015 NIBRS Crime Data Released: Report Contains More Detail on Criminal Offenses, page 132

CYBER CRIMES

Lottery Fraud: Scammers Target the Elderly, page 25

Syrian Cyber Hackers Charged: Two From 'Syrian Electronic Army' Added to Cyber's Most Wanted, page 29

International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector, pages 30-31

A Web of Intimidation: Landmark Cyberstalking Case Results in Life Sentences for Three Family Members, page 38

Sextortion and Cyberstalking: How a Single Tip Uncovered an International Scheme, page 42

Incidents of Ransomware on the Rise: Protect Yourself and Your Organization, pages 43-44

Index

Child Sexual Exploitation: Threat from Pedophiles Online is ‘Vast and Extensive’, page 50

Countering the Cyber Threat
New U.S. Cyber Security Policy
Codifies Agency Roles, page 78

Victimized by a Cyber Scammer?
Don’t Forget to File a Complaint
with the IC3, page 80

Take the Safe Online Surfing
Internet Challenge: Available
Soon for 2016-2017 School Year,
page 89

National Cyber Security Awareness
Month: Cyber Security is
Everyone’s Responsibility,
page 108

National Cyber Security Awareness
Month: Simple Steps for Internet
Safety, page 109

National Cyber Security Awareness
Month: FBI, Partners, Offer
Online Cyber Training for Law
Enforcement First Responders,
page 113

National Cyber Security Awareness
Month: FBI Deploys Cyber
Experts to Work Directly with
Foreign Partners, page 115

A Primer on DarkNet
Marketplaces: What They are
and What Law Enforcement is
Doing to Combat Them, pages
116-117

Cyber Operation Takes Down
Avalanche Criminal Network:
Servers Enabled Nefarious
Activity Worldwide, page 127

International Cyber Sweep Nets
DDoS Attackers: California Grad
Student Arrested in Operation
Aimed at Young Hackers,
page 133

DIRECTOR/FBI LEADERSHIP

FBI Recognizes Leaders from
Around the Nation: Director’s
Community Leadership Awards
Presented, page 39

Civil Rights and Law Enforcement:
Director Speaks at Birmingham
Conference, pages 56-57

Oil and Crime in Indian Country:
Director Visits Reservation in
North Dakota to Discuss Rising
Threat, page 59

Director Provides Update
on Orlando Shootings
Investigations, page 61

FIELD CASES

Fool’s Gold: Company That
Enabled Get-Rich-Quick
Schemes Left Many High and
Dry, page 1

Financial Fraud: The Disney
Resort That Never Was, page 8

Operation Ghost Guard:
Widespread Public Corruption
Inside Georgia Prisons,
pages 16-17

Egg Donation and Surrogacy Scam:
California Woman Robbed
Would-Be Parents of Money and
Hope, page 18

Counterfeit Cabs: Auto Broker
Who Used Salvage Vehicles as
Taxis Sentenced, page 19

Caught in the Act: Prolific
Washington State Bank Robber
Sent to Prison, page 20

Putting the Brakes on Crime:
Getaway Driver Sentenced to 121
Years, page 21

A Wartime Loss Found: FBI
Assists Polish Government in
Recovering Painting Lost During
WWII, pages 23-24

Lottery Fraud: Scammers Target
the Elderly, page 25

Arkansas Drug Trafficking
Enterprise Dismantled: Leader
Gets 20 Years in Prison After
Multi-Agency Investigation,
page 26

Food Stamp Fraud: Supermarket
Owner Imprisoned for Multi-
Million-Dollar Scam, page 27

Check-Cashing Scheme Voided:
Multi-Agency Effort Disrupts
U.S. Treasury Check-Cashing
and Identity Theft Ring, page 28

A Look Back at the Coors
Kidnapping Case: Law
Enforcement Collaboration and
Public Assistance Played Key
Role, pages 32-33

Financial Fraud: Pharmaceutical
Executive Sold Fake Stock in
Medical Research Company,
page 34

New Top Ten Fugitive: Help Us
Find a Murderer, page 35

Wind Farm Investment Scam:
Texas Man Sentenced to 15
Years in Federal Prison,
pages 36-37

A Web of Intimidation: Landmark
Cyberstalking Case Results in
Life Sentences for Three Family
Members, page 38

Man Gets 16 Years for Attempting
to Purchase Ricin: Use of Stolen
Identity Adds to Length of
Sentence, page 40

Violent Home Invasion: Case
Illustrates Threat Posed by
Gangs, page 41

Sextortion and Cyberstalking:
How a Single Tip Uncovered an
International Scheme, page 42

Countering Terrorism: Inside the
Mufid Elfgeeh Investigation,
page 52

New Top Ten Fugitives: Help Us
Find Two Murderers, page 53

Index

Child Sex Tourism: Alaska Man
Receives Prison Term for Crimes
Committed in Cambodia,
page 55

Darwin Letter Recovered: FBI
Returns 1875 Correspondence to
Smithsonian Archives, page 58

Animal Rights Extremists: Pair
Took Law into Their Own
Hands, page 60

Cold Case Killer: Help Us Catch
the East Area Rapist, pages 62-63

Taking Flight: Man Sentenced
for Distributing Avionics Trade
Secrets, page 64

Taken Hostage: Mexican Drug
Cartel Influence Felt in Rural
South Carolina, page 65

Intellectual Property Crime:
Trio Pirated Mercedes-Benz
Diagnostic Software, page 66

New Top Ten Fugitive: Help Us
Catch a Murderer, page 67

Electronics Smuggler Sentenced:
Sensitive Equipment Illegally
Exported to Russia, page 70

The Long Hike to Prison: Fugitive
Spent Years Hiding on the
Appalachian Trail, page 72

Health Care Fraud: Three Charged
in \$1 Billion Medicare Fraud
Scheme, page 75

'A Predator in Every Sense of the
Word': Subject Gets 70 Years for
Theft Scheme and Producing
Child Pornography, page 79

Health Care Fraud: Service
Provider's Crimes Caused
Patients' Deaths, page 81

First Federal Spoofing Prosecution:
Trader Sentenced in Case
Involving Manipulation of
Market Prices, page 82

Murder for Hire: Alaska Man
Wanted Federal Agents Killed,
page 83

Fugitive Apprehended: Alleged
Child Abuser Was on the Run
for 23 Years, page 88

1991 Talladega Prison Riot: A
Look Back at the FBI's Early
Crisis Response Capabilities,
pages 90-91

Chicago Cold Case: Seeking Justice
for a Murdered Teenage Girl,
page 92

Human Trafficking: Guatemalan
Migrants Exploited in Forced
Labor Scheme, page 95

Animal Cruelty: Houston 'Crush'
Cases Were First Under Federal
Statute, page 106

Public Corruption: Chicago
Transportation Official Took
Bribes for a Decade, pages
118-119

Burglary Crew: Break-In Netted
'Jedi Knight' Thieves \$2.5
Million in Jewels, page 120

A Legacy of Crime Brought to an
End: Violent Gang Leader in
Buffalo Sentenced for Role in
Murders, page 121

Con Artist Brought to Justice:
Arizona Woman Faked Cancer,
Scammed Veterans, page 123

New Top Ten Fugitive: Help Us
Catch a Murderer, page 126

International Cyber Sweep Nets
DDoS Attackers: California Grad
Student Arrested in Operation
Aimed at Young Hackers,
page 133

New Top Ten Fugitive: Help Us
Capture a Murderer, page 134

New Top Ten Fugitive: Help Us
Catch a Killer, page 135

Protecting Vital Assets: Pilfering
of Corn Seeds Illustrates
Intellectual Property Theft,
pages 136-137

FOREIGN COUNTERINTELLIGENCE

Countering the Growing
Intellectual Property Theft
Threat: Enhancing Ties Between
Law Enforcement and Business,
page 9

Taking Flight: Man Sentenced
for Distributing Avionics Trade
Secrets, page 64

Electronics Smuggler Sentenced:
Sensitive Equipment Illegally
Exported to Russia, page 70

Protecting Vital Assets: Pilfering
of Corn Seeds Illustrates
Intellectual Property Theft,
pages 136-137

A Look Back: A Small Office with
a Big Mission: The FBI's World
War II-Era Cover Company at
Rockefeller Center, pages 140-141

HISTORY

A Look Back at the Coors
Kidnapping Case: Law
Enforcement Collaboration and
Public Assistance Played Key
Role, pages 32-33

Artifact of the Month: Historical
Items Featured on FBI Social
Media Accounts, page 85

1991 Talladega Prison Riot: A
Look Back at the FBI's Early
Crisis Response Capabilities,
pages 90-91

Remembering 9/11: FBI Has
Evolved in Response to Changing
Threats, page 94

A Look Back: A Small Office with
a Big Mission: The FBI's World
War II-Era Cover Company at
Rockefeller Center, pages 140-141

Index

INTELLIGENCE

Training Together: New FBI Academy Program Integrates Agents and Intelligence Analysts, pages 10-11

Identifying the Vulnerabilities: Weapons of Mass Destruction Directorate Marks 10 Years, pages 76-77

INTERNATIONAL

Transnational Gangs, Part 1: Understanding the Threat, pages 2-3

Transnational Gangs, Part 2: Countering the Threat with Strong Partnerships, pages 4-5

Transnational Gangs, Part 3: Investigators and Prosecutors Join Forces, pages 6-7

A Wartime Loss Found: FBI Assists Polish Government in Recovering Painting Lost During WWII, pages 23-24

Syrian Cyber Hackers Charged: Two From 'Syrian Electronic Army' Added to Cyber's Most Wanted, page 29

International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector, pages 30-31

Sextortion and Cyberstalking: How a Single Tip Uncovered an International Scheme, page 42

Child Sex Tourism: Alaska Man Receives Prison Term for Crimes Committed in Cambodia, page 55

Electronics Smuggler Sentenced: Sensitive Equipment Illegally Exported to Russia, page 70

International Corruption: U.S. Seeks to Recover \$1 Billion in Largest Kleptocracy Case to Date, pages 73-74

Report from Thailand, Part 1: Confronting the Child Sex Trade in Southeast Asia, pages 96-97

Report from Thailand, Part 2: A New Emphasis on Helping Child Victims, pages 98-99

Report from Thailand, Part 3: It Takes a Village, pages 100-101

Report from Thailand, Part 4: Strengthening Investigations Through Collaboration, pages 102-103

Operation Cross Country X: Recovering Underage Victims of Sex Trafficking and Prostitution, pages 110-111

Combating the Growing Money Laundering Threat: Specialized FBI Unit Focuses on Disrupting Professional Money Launderers, page 114

National Cyber Security Awareness Month: FBI Deploys Cyber Experts to Work Directly with Foreign Partners, page 115

International Contract Fraud: U.S. Government Employee Steered \$2 Million in Micro-Dairy Contracts to His Son, pages 124-125

Cyber Operation Takes Down Avalanche Criminal Network: Servers Enabled Nefarious Activity Worldwide, page 127

On the Waterfront: Task Force Works to Stem Flow of Illicit Drug Trafficking and Dismantle Criminal Networks, pages 128-131

International Cyber Sweep Nets DDoS Attackers: California Graduate Student Arrested in Operation Aimed at Young Hackers, page 133

Corruption on the Border: New Campaign Enlists the Public's Help, pages 138-139

LAB/OPERATIONAL TECHNOLOGY

Forensic Anthropology: Laboratory Artist Puts a Human Face on Unidentified Remains, pages 68-69

1991 Talladega Prison Riot: A Look Back at the FBI's Early Crisis Response Capabilities, pages 90-91

MAJOR THEFTS/VIOLENT CRIME

Transnational Gangs, Part 1: Understanding the Threat, pages 2-3

Transnational Gangs, Part 2: Countering the Threat with Strong Partnerships, pages 4-5

Transnational Gangs, Part 3: Investigators and Prosecutors Join Forces, pages 6-7

Tracking Animal Cruelty: FBI Collecting Data on Crimes Against Animals, page 12

Caught in the Act: Prolific Washington State Bank Robber Sent to Prison, page 20

Putting the Brakes on Crime: Getaway Driver Sentenced to 121 Years, page 21

New Top Ten Fugitive: Help Us Find a Murderer, page 35

A Web of Intimidation: Landmark Cyberstalking Case Results in Life Sentences for Three Family Members, page 38

Violent Home Invasion: Case Illustrates Threat Posed by Gangs, page 41

Violent Criminal Apprehension Program, Part 1: Sharing Information to Stop Serial Offenders, pages 45-47

Index

Violent Criminal Apprehension Program, Part 2: The Highway Serial Killings Initiative, pages 48-49

New Top Ten Fugitives: Help Us Find Two Murderers, page 53

Oil and Crime in Indian Country: Director Visits Reservation in North Dakota to Discuss Rising Threat, page 59

Cold Case Killer: Help Us Catch the East Area Rapist, pages 62-63

Taken Hostage: Mexican Drug Cartel Influence Felt in Rural South Carolina, page 65

New Top Ten Fugitive: Help Us Catch a Murderer, page 67

'A Predator in Every Sense of the Word': Subject Gets 70 Years for Theft Scheme and Producing Child Pornography, page 79

Murder for Hire: Alaska Man Wanted Federal Agents Killed, page 83

FBI Releases New Bank Robbers Mobile App: Asking for Help in Identifying Unknown Suspects, pages 86-87

Chicago Cold Case: Seeking Justice for a Murdered Teenage Girl, page 92

Latest Crime Statistics Released: Increase in Violent Crime, Decrease in Property Crime, page 105

Animal Cruelty: Houston 'Crush' Cases Were First Under Federal Statute, page 106

LEOKA Report Released: 41 Officers Feloniously Killed in 2015, page 112

Burglary Crew: Break-In Netted 'Jedi Knight' Thieves \$2.5 Million in Jewels, page 120

A Legacy of Crime Brought to an End: Violent Gang Leader in Buffalo Sentenced for Role in Murders, page 121

New Top Ten Fugitive: Help Us Catch a Murderer, page 126

2015 NIBRS Crime Data Released: Report Contains More Detail on Criminal Offenses, page 132

New Top Ten Fugitive: Help Us Capture a Murderer, page 134

New Top Ten Fugitive: Help Us Catch a Killer, page 135

ORGANIZED CRIME/DRUGS

Transnational Gangs, Part 1: Understanding the Threat, pages 2-3

Transnational Gangs, Part 2: Countering the Threat with Strong Partnerships, pages 4-5

Transnational Gangs, Part 3: Investigators and Prosecutors Join Forces, pages 6-7

Raising Awareness of Opioid Addiction: FBI, DEA Release Documentary Aimed at Youth, page 13

Arkansas Drug Trafficking Enterprise Dismantled: Leader Gets 20 Years in Prison After Multi-Agency Investigation, page 26

Violent Home Invasion: Case Illustrates Threat Posed by Gangs, page 41

Taken Hostage: Mexican Drug Cartel Influence Felt in Rural South Carolina, page 65

'A Predator in Every Sense of the Word': Subject Gets 70 Years for Theft Scheme and Producing Child Pornography, page 79

A Legacy of Crime Brought to an End: Violent Gang Leader in Buffalo Sentenced for Role in Murders, page 121

On the Waterfront: Task Force Works to Stem Flow of Illicit Drug Trafficking and Dismantle Criminal Networks, pages 128-131

PARTNERSHIPS

Transnational Gangs, Part 1: Understanding the Threat, pages 2-3

Transnational Gangs, Part 2: Countering the Threat with Strong Partnerships, pages 4-5

Transnational Gangs, Part 3: Investigators and Prosecutors Join Forces, pages 6-7

Countering the Growing Intellectual Property Theft Threat: Enhancing Ties Between Law Enforcement and Business, page 9

Arkansas Drug Trafficking Enterprise Dismantled: Leader Gets 20 Years in Prison After Multi-Agency Investigation, page 26

Oil and Crime in Indian Country: Director Visits Reservation in North Dakota to Discuss Rising Threat, page 59

Countering the Cyber Threat New U.S. Cyber Security Policy Codifies Agency Roles, page 78

Report from Thailand, Part 1: Confronting the Child Sex Trade in Southeast Asia, pages 96-97

Report from Thailand, Part 2: A New Emphasis on Helping Child Victims, pages 98-99

Report from Thailand, Part 3: It Takes a Village, pages 100-101

Report from Thailand, Part 4: Strengthening Investigations Through Collaboration, pages 102-103

Index

Hazardous Devices School: FBI Takes Lead Role in Training Nation's Public Safety Bomb Technicians, page 104

Operation Cross Country X: Recovering Underage Victims of Sex Trafficking and Prostitution, pages 110-111

National Cyber Security Awareness Month: FBI, Partners, Offer Online Cyber Training for Law Enforcement First Responders, page 113

National Cyber Security Awareness Month: FBI Deploys Cyber Experts to Work Directly with Foreign Partners, page 115

A Primer on DarkNet Marketplaces: What They are and What Law Enforcement is Doing to Combat Them, pages 116-117

Cyber Operation Takes Down Avalanche Criminal Network: Servers Enabled Nefarious Activity Worldwide, page 127

On the Waterfront: Task Force Works to Stem Flow of Illicit Drug Trafficking and Dismantle Criminal Networks, pages 128-131

International Cyber Sweep Nets DDoS Attackers: California Grad Student Arrested in Operation Aimed at Young Hackers, page 133

Corruption on the Border: New Campaign Enlists the Public's Help, pages 138-139

PUBLIC/COMMUNITY OUTREACH

Raising Awareness of Opioid Addiction: FBI, DEA Release Documentary Aimed at Youth, page 13

Countering Violent Extremism: FBI Launches New Awareness Program for Teens, pages 14-15

FBI Tip Line: Web Portal, Created in 2001, Receives 'Actionable' Tips Daily, page 22

Syrian Cyber Hackers Charged: Two From 'Syrian Electronic Army' Added to Cyber's Most Wanted, page 29

International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector, pages 30-31

New Top Ten Fugitive: Help Us Find a Murderer, page 35

FBI Recognizes Leaders from Around the Nation: Director's Community Leadership Awards Presented, page 39

Human Rights: FBI Reaching Out About Female Genital Mutilation, page 51

New Top Ten Fugitives: Help Us Find Two Murderers, page 53

Help Us Find Them: National Missing Children's Day 2016, page 54

Cold Case Killer: Help Us Catch the East Area Rapist, pages 62-63

New Top Ten Fugitive: Help Us Catch a Murderer, page 67

Finding Solace: FBI Crisis Response Canines Help Victims Cope with Tragedy, page 71

Victimized by a Cyber Scammer? Don't Forget to File a Complaint with the IC3, page 80

FBI Releases New Bank Robbers Mobile App: Asking for Help in Identifying Unknown Suspects, pages 86-87

Take the Safe Online Surfing Internet Challenge: Available Soon for 2016-2017 School Year, page 89

Chicago Cold Case: Seeking Justice for a Murdered Teenage Girl, page 92

Future Agents in Training: High School Students Get Inside Look at FBI Careers, page 93

National Cyber Security Awareness Month: Cyber Security is Everyone's Responsibility, page 108

National Cyber Security Awareness Month: Simple Steps for Internet Safety, page 109

New Top Ten Fugitive: Help Us Catch a Murderer, page 126

New Top Ten Fugitive: Help Us Capture a Murderer, page 134

New Top Ten Fugitive: Help Us Catch a Killer, page 135

PUBLIC CORRUPTION

Operation Ghost Guard: Widespread Public Corruption Inside Georgia Prisons, pages 16-17

International Corruption: U.S. Seeks to Recover \$1 Billion in Largest Kleptocracy Case to Date, pages 73-74

Public Corruption: Chicago Transportation Official Took Bribes for a Decade, pages 118-119

International Contract Fraud: U.S. Government Employee Steered \$2 Million in Micro-Dairy Contracts to His Son, pages 124-125

Corruption on the Border: New Campaign Enlists the Public's Help, pages 138-139

RECRUITING/DIVERSITY

Training Together: New FBI Academy Program Integrates Agents and Intelligence Analysts, pages 10-11

Index

Forensic Anthropology: Laboratory Artist Puts a Human Face on Unidentified Remains, pages 68-69

Cadre of Special Agent Candidates Gathers in D.C.: Recruiting Event Supports FBI Commitment to a Diverse Workforce, page 84

Future Agents in Training: High School Students Get Inside Look at FBI Careers, page 93

Team USA Athletes Welcomed by FBI: Bureau Holds Career Information Session for Olympians and Paralympians, page 107

TECHNOLOGY

FBI Releases New Bank Robbers Mobile App: Asking for Help in Identifying Unknown Suspects, pages 86-87

TRAINING

Training Together: New FBI Academy Program Integrates Agents and Intelligence Analysts, pages 10-11

Violent Criminal Apprehension Program, Part 1: Sharing Information to Stop Serial Offenders, pages 45-47

Violent Criminal Apprehension Program, Part 2: The Highway Serial Killings Initiative, pages 48-49

Report from Thailand, Part 1: Confronting the Child Sex Trade in Southeast Asia, pages 96-97

Report from Thailand, Part 2: A New Emphasis on Helping Child Victims, pages 98-99

Report from Thailand, Part 3: It Takes a Village, pages 100-101

Report from Thailand, Part 4: Strengthening Investigations Through Collaboration, pages 102-103

Hazardous Devices School: FBI Takes Lead Role in Training Nation's Public Safety Bomb Technicians, page 104

National Cyber Security Awareness Month: FBI, Partners, Offer Online Cyber Training for Law Enforcement First Responders, page 113

WHITE-COLLAR CRIME

Fool's Gold: Company That Enabled Get-Rich-Quick Schemes Left Many High and Dry, page 1

Financial Fraud: The Disney Resort That Never Was, page 8

Countering the Growing Intellectual Property Theft Threat: Enhancing Ties Between Law Enforcement and Business, page 9

Egg Donation and Surrogacy Scam: California Woman Robbed Would-Be Parents of Money and Hope, page 18

Counterfeit Cabs: Auto Broker Who Used Salvage Vehicles as Taxis Sentenced, page 19

Lottery Fraud: Scammers Target the Elderly, page 25

Food Stamp Fraud: Supermarket Owner Imprisoned for Multi-Million-Dollar Scam, page 27

Check-Cashing Scheme Voided: Multi-Agency Effort Disrupts U.S. Treasury Check-Cashing and Identity Theft Ring, page 28

Financial Fraud: Pharmaceutical Executive Sold Fake Stock in Medical Research Company, page 34

Wind Farm Investment Scam: Texas Man Sentenced to 15 Years in Federal Prison, pages 36-37

Taking Flight: Man Sentenced for Distributing Avionics Trade Secrets, page 64

Intellectual Property Crime: Trio Pirated Mercedes-Benz Diagnostic Software, page 66

The Long Hike to Prison: Fugitive Spent Years Hiding on the Appalachian Trail, page 72

International Corruption: U.S. Seeks to Recover \$1 Billion in Largest Kleptocracy Case to Date, pages 73-74

Health Care Fraud: Three Charged in \$1 Billion Medicare Fraud Scheme, page 75

Health Care Fraud: Service Provider's Crimes Caused Patients' Deaths, page 81

First Federal Spoofing Prosecution: Trader Sentenced in Case Involving Manipulation of Market Prices, page 82

Combating the Growing Money Laundering Threat: Specialized FBI Unit Focuses on Disrupting Professional Money Launderers, page 114

Con Artist Brought to Justice: Arizona Woman Faked Cancer, Scammed Veterans, page 123

International Contract Fraud: U.S. Government Employee Steered \$2 Million in Micro-Dairy Contracts to His Son, pages 124-125

FBI OFFICE OF PUBLIC AFFAIRS

935 Pennsylvania Avenue NW

Washington, D.C. 20535



The crew of a self-propelled semi-submersible (SPSS) vessel prepares to abandon their boat before being intercepted and detained by the Coast Guard northwest of the Colombia-Ecuador border in 2009. (U.S. Coast Guard photo)