U.S. Department of Justice
Federal Bureau of Investigation

2014 The FBI Story

FBI Director James B. Comey speaks to Cyber Division employees at FBI Headquarters.

2014 The FBI Story

www.fbi.gov

The National Cyber Investigative Joint Task Force is composed of nearly two dozen federal intelligence, military, and law enforcement agencies, along with local law enforcement and international and private industry partners. The task force serves as the government's central hub for coordinating, integrating, and sharing information related to cyber threat investigations.

A Message from FBI Director James B. Comey

It has been a busy and challenging year for the FBI and for our partners at home and around the world. Together, we confronted cyber attacks from sophisticated, state-sponsored actors, transnational criminal groups, and everyday hackers. We arrested white-collar criminals and corrupt public officials. We protected our communities from violent gangs and child predators. And we safeguarded Americans from an array of counterterrorism and counterintelligence threats.

This latest edition of *The FBI Story*, our annual collection of news and feature articles from our public website, FBI.gov, chronicles our most successful 2014 investigations and operations. These include the disruption of botnet operators responsible for the theft of more than $100 million worldwide; nearly $9 billion in penalties levied against one of the largest financial institutions in the world for exploiting the American financial system; and a nationwide child exploitation sweep that recovered 168 victims of trafficking.

This edition of *The FBI Story* also highlights some of our unique capabilities. You will find multi-part series on gangs and serial killers, as well as features on the biometric system known as Next Generation Identification (now fully operational) and the completion of a project to digitize FBI files, including 30 million records and 83 million fingerprint cards. You will also find historical pieces on Benson House, which played a crucial role in our counterintelligence operations during World War II, and the 50th anniversary of the investigation into the disappearance of three civil rights workers in Mississippi in 1964—a case widely known as Mississippi Burning.

Our work to protect the United States and its citizens never stops. As these stories make clear, we don't operate in isolation. We need our federal, state, local, tribal, and international law enforcement and intelligence partners—as well as our non-governmental and private sector allies—to succeed. We also need the trust and cooperation of the American people. Without your assistance, our mission would be far more difficult.

I've been FBI Director for more than a year, and I believe—now, more than ever—that the FBI is an amazing organization. We have folks doing an astonishing array of things all over the world, and doing them well. But we can't do those things without your support. On behalf of the entire FBI, I hope you enjoy this latest edition of *The FBI Story*. We look forward to working with you—and for you—in 2015.

James B. Comey

Director Comey discusses the impact of emerging technology on public safety in a speech at the Brookings Institution in Washington, D.C.

Counterfeit Cosmetics, Fragrances

Hazardous to Your Health

You see what appears to be your favorite brand name eye shadow, eye liner, or fragrance for sale at a flea market or on an unfamiliar website. You notice the price is lower than what you normally pay at your favorite retail store or through an authorized online dealer.

Before you hand over your hard-earned money, though, keep this in mind: It could be counterfeit, and—in addition to buying something that's not the real deal—you are also risking your health by buying and using products that may contain substandard or even dangerous substances.

The National Intellectual Property Rights (IPR) Center—of which the FBI is a partner—wants you to know that the volume of all sorts of counterfeit cosmetics and fragrances coming into the U.S. is definitely on the rise…that's according to our industry partners as well as law enforcement. Why is this happening? Because the Internet has given counterfeiters widespread access to customers, and because criminals increasingly view dealing in counterfeit personal care products—as well as other knock-off consumer goods as well—as a relatively low-risk crime since many of the perpetrators are located outside of the U.S.

Government and industry studies and testing have discovered that some of the ingredients that make up counterfeit cosmetics and fragrances are downright dangerous:

- Phony cosmetics often contain things such as arsenic, beryllium, and cadmium (all known carcinogens) along with high levels of aluminum and dangerous levels of bacteria. Some of these products have caused conditions like acne, psoriasis, rashes, and eye infections.
- Counterfeit fragrances have been found to contain something called DEHP, classified by the Environmental Protection Agency as a probable human carcinogen. These phony perfumes and colognes, which sometimes contain urine as well, have been known to cause serious skin rashes.

There is no typical profile of the individuals or groups trafficking in these kinds of counterfeit products…and this might just be one of their many illegal activities—

often times, the illicit proceeds are used to fund other types of crime. We've also seen people selling counterfeit products through online auction sites and other websites just to make a little extra cash…some may not even realize their merchandise is fake.

Because of the dangers to the public, law enforcement is mobilizing against counterfeit cosmetics and fragrances. For example, the nearly two dozen U.S. and foreign agencies that make up the National IPR Center are working on the matter—sharing intelligence with one another, coordinating with state and local law enforcement, and developing relationships with industry representatives.

But we need the public's help.

First, educate yourself about some of the common indicators of counterfeit cosmetics and fragrances so that you don't become a victim. If you're not sure about the authenticity of a product, don't buy it.

And second, if you think you or someone you know may have purchased counterfeit cosmetics or fragrances—or if you suspect someone of selling counterfeit items—submit a tip to the National IPR Center. The more information law enforcement has, the more effective we can be. With the proliferation of counterfeit goods increasing at an alarming rate, the National IPR Center focuses on keeping these bogus and often unsafe products off U.S. streets while dismantling the criminal organizations behind this activity.

On the Ground in Kenya

Part 1: A Conversation with Our Legal Attaché in Nairobi

The FBI's legal attaché, or legat, program places Bureau personnel in more than 60 countries around the world. Working primarily through U.S. Embassies, our employees serve at the pleasure of host country governments, and their core mission is to establish and maintain liaison with local law enforcement and security services. Such partnerships are critical in the fight against international terrorism, cyber crime, and a range of other criminal and intelligence matters.

FBI.gov recently sat down with Dennis Brady, the Bureau's legal attaché in Nairobi, Kenya, to talk about our partnerships with the Kenyans and our work in that region of the world.

Q: What are the key threats in Kenya that impact Americans and U.S. interests?

Brady: The terrorist organization al Shabaab has been the biggest threat we face. Members of that group use IEDs [improvised explosive devices] to carry out terrorist attacks. They are known to throw grenades into local buses and attack local police officers. They also have a history of kidnapping Americans in Somalia—an area that our legat office covers. Piracy in Somalia is also a continuing threat.

Q: What types of FBI personnel are posted to Legat Nairobi?

Brady: In addition to our administrative and support staff, we have a special agent bomb technician, a member of the FBI's counterterrorism fly team, and a Hostage Rescue Team operator embedded on a permanent rotating basis. So when something happens—a kidnapping or an act of terror or piracy—we can respond immediately with a full range of Bureau expertise.

Q: Is that expertise also used to help train Kenyan law enforcement?

Brady: Absolutely. Training is one of our key functions, and it's been going on for years. We train Kenyan law enforcement personnel in a variety of disciplines, including crime scenes, IEDs, and tactics. We also provide instruction in areas such as fingerprinting, cyber investigations, evidence collection, intelligence analysis, interview techniques, and major case management. In the past few years, the Bureau has conducted more than 40 training sessions in Kenya and has trained more than 800 individuals. We also have 10 Kenyan graduates of the FBI's National Academy who are still active in law enforcement. The Kenyans are very receptive to everything we offer and are enthusiastic, active participants in the process. What we provide supplements their own training and significantly improves their capacity to do their jobs.

Q: Does the training have other benefits?

Brady: Yes, it further strengthens our working relationship with the Kenyans and reminds us of how much we have in common. Kenya was formerly a British colony and has a European-style legal system. The police and defense forces are separate, and the country operates its law enforcement and courts under the rule of law. Kenya also has an extradition treaty with the U.S., so when we locate fugitives, we can get them removed through the legal process and extradited back to the U.S. to face justice. All of these things make for good partnerships, and that becomes critical when you are responding to a crisis like the Westgate Mall terror attack a few months ago. In a life and death situation like that, everyone needs to know they can rely on one another.

Part 2: Terror at the Westgate Mall (page 3)

On the Ground in Kenya

Part 2: Terror at the Westgate Mall

Part 2 of an interview with Dennis Brady, the FBI's legal attaché in Nairobi, Kenya.

Q: On September 21, 2013, al Shabaab gunmen attacked the Westgate shopping mall in Nairobi. Over a period of several days, they killed more than 70 people. What was the FBI's response?

Brady: The attack started on a Saturday. I was called to the embassy, and we immediately began securing resources to assist the Kenyans. Our people were on the scene from the first day. The FBI's role was—and continues to be—to facilitate, enable, and assist the Kenyan investigation and prosecution regarding a crime that occurred largely against Kenyan citizens on their soil.

Q: After the attack ended, what was the crime scene like?

Brady: Very complicated. Westgate was a large mall, four stories, with underground parking and an attached parking structure. In the process of fighting the attackers, there were explosions and a fire. The area where the attackers were had home furnishings that caught fire. The fire spread and continued to burn, causing that part of the structure to collapse into a pit that smoldered for weeks.

Q: Was it dangerous for investigators working to collect evidence?

Brady: It's amazing we got our Evidence Response Team [ERT] people down into that pit. It was a very difficult place to work. While ERT was doing its work, every now and then a propane tank would explode or vehicles on the edge of the collapse would fall in and catch fire. But there was a lot of attention paid to the soundness of the structure and where we could reasonably collect evidence. Safety of the investigators was paramount. We had an FBI structural engineer and hazardous materials experts on scene in addition to our other assets. At the height of the initial investigation, the Bureau had more than 80 people on the ground there.

Q: Where does the investigation stand now?

Brady: The Kenyans have charged four individuals in connection with the terror attack, and the case is moving through the court process. The four are directly

connected to the individuals who physically carried out the attack. Nobody is under the impression that we have fully identified the entire network in this attack, however. That's why the investigation continues.

Q: There have been conflicting reports about what happened to the gunmen. Can you comment?

Brady: We believe, as do the Kenyan authorities, that the four gunmen inside the mall were killed. Our ERT made significant finds, and there is no evidence that any of the attackers escaped from the area where they made their last stand. Three sets of remains were found. Also, the Kenyans were on the scene that first day and set up a very secure crime scene perimeter, making an escape unlikely. Additionally, had the attackers escaped, it would have been publicly celebrated and exploited for propaganda purposes by al Shabaab. That hasn't happened.

Q: All in all, are you pleased with how the legat responded to the crisis?

Brady: Very much so. Our people stood shoulder to shoulder with the Kenyans through some very difficult days. It's also worth noting that it wasn't just Americans helping the Kenyans. It was an international effort. But yes, I am proud of how the legat responded and how we were able to assist our host country when they most needed us.

Serial Killers

Part 4: White Supremacist Joseph Franklin

It was a deadly mix: a mentally troubled man from an abusive, broken home turned radical racist and then serial killer.

His name was Joseph Paul Franklin, and he went on a horrific killing spree beginning in 1977 at the age of 27. Before his reign of murder ended in 1980, he took the lives of at least 15 men, women, and children in some 11 states. He also admitted shooting civil rights leader Vernon Jordan and paralyzing pornography publisher Larry Flynt.

Franklin was drawn to white supremacist ideologies as a teen. Dropping out of high school following a severe eye injury, he got married, became an abusive husband, and began racking up minor legal violations.

As his association with white supremacist groups grew, Franklin became increasingly confrontational toward minorities. By the mid-1970s, he had rejected even the most radical hate groups because he didn't think they took their hatred far enough. His self-directed "mission," he later suggested, was to incite his fellow supremacists to action.

Left: Joseph Paul Franklin (Missouri Department of Corrections Photo)

The summer of 1976 marked a turning point. On Labor Day weekend in Atlanta, Franklin followed an interracial couple and sprayed them with mace. This was his first known physical attack…it escalated from there. On July 29, 1977, he bombed a Tennessee synagogue; a few days later in Wisconsin, he killed two men—one black and one white—after encountering them in a parking lot.

For the next three years, Franklin drifted across the country, robbing banks and using a sniper rifle to target his victims. He killed possibly more than 20 people and seriously injured six more.

By 1980, the FBI and its partners were closing in on Franklin. The often vast miles and lack of evidentiary connections between his crimes—as well as his skill at living the life of an anonymous drifter—kept Franklin under the radar for a time. This changed in September 1980, when an observant police officer in Kentucky noticed a gun in the back of a car Franklin was driving. A records check showed an outstanding warrant, and Franklin was brought in for questioning. He escaped while being detained, but the Bureau was on his trail.

Evidence from the car suggested multiple connections to the racially motivated sniper attacks across the country. The Bureau's behavioral analysts contributed their insights, and the FBI shared its growing knowledge of Franklin's characteristics and tactics with law enforcement and the public. Two details were crucial—Franklin's racist tattoos and his reliance on blood bank donations for cash while between bank robberies.

Within weeks, a blood-bank operator in Florida contacted the Bureau about a man matching Franklin's description. FBI agents immediately tracked him to Lakeland, Florida and arrested him on October 28, 1980.

Franklin faced legal action across the U.S. for the next two decades, eventually being convicted of multiple murders, attacks, and other crimes. He was sentenced to life in prison and received the death penalty in several states. On November 11, 2013, he was executed in Missouri for the 1977 murder of a man standing in front of a synagogue in St. Louis.

Note: Parts 1-3 of this series were published in 2013.

Part 5: Wayne Williams and the Atlanta Child Murders (page 11)

Prepaid Funeral Scam

Fitting End to Multi-State Fraud Scheme

Scamming nuns. Taking advantage of the mentally disabled. Stealing from the elderly. Just when you think con men couldn't sink any lower, they do: This time, a group of fraudsters took money from individuals who prepaid their own funerals to ease the financial and emotional burdens on their families.

Recently, a Missouri man and five others were sentenced to federal prison for their role in a Ponzi-like prepaid funeral scheme that victimized some 97,000 customers in more than 16 states. The scheme caused more than $450 million in losses, smaller or non-existent death benefits for families at their most vulnerable, and huge profits that lined the pockets of the defendants.

According to the Federal Trade Commission, millions of Americans enter into contracts to prearrange their funerals and prepay some or all of the expenses involved. Laws in individual states regulate the industry, and various states have laws to help ensure that these advance payments are available when they're needed. However, protections vary widely from state to state, sometimes providing a window of opportunity for unscrupulous operators.

That's just what happened with James "Doug" Cassity and his Missouri-based company called National Prearranged Services Inc. (NPS). As early as 1992 and until 2008, Cassity and the other defendants employed by NPS or affiliated life insurance companies devised and ran a scheme to defraud purchasers of prearranged funeral contracts obtained from NPS. Also victimized were funeral homes that did business with NPS, financial institutions that served as trustees of the prearranged trusts established by NPS for their customers, and state insurance guarantee associations.

In general, here's what NPS told its customers: After discussing what the customer wanted, a price would be agreed upon and payment accepted. NPS would make arrangements with the customer-designated funeral home. In accordance with state law, the funds would be placed with a third party—depending on the state, that third party would be a financial institution that would put the funds into a trust that could be only used for safe investments (like government-backed securities)…or a life insurance company that would put the funds into a life insurance policy in the name of the customer.

Here's what NPS didn't tell its customers: The company didn't put all of the funds from customers into a trust or life insurance policy, but instead brazenly altered application documents—i.e., changing deposit amounts, naming itself as a beneficiary, converting whole life insurance policies to term life—and used the money for unauthorized purposes like risky investments, payments for existing funeral claims, and personal enrichment. In some instances, defendants even removed money previously placed in trusts and life insurance policies. And NPS routinely lied to state regulators about its practices.

And if that wasn't bad enough, NPS also purchased large blocks of prearranged funeral contracts from funeral homes that had previously entered into their own prearranged funeral contracts with customers, falsely telling these funeral homes that the contracts would be rolled over into life insurance policies.

The complex case—investigated by three federal agencies, a number of state regulatory agencies, and the Department of Justice—began in 2008 when we received information from several state agencies on the shady practices of NPS and one of its affiliated life insurance companies. It ended in November 2013, when six co-conspirators who took advantage of people's desire to protect their loved ones upon their own deaths were finally brought to justice.

Scam on the Run

Fugitive Identity Thief Led Global Criminal Enterprise

He made a living stealing other people's identities…and then their money. And what a living it was—more than enough to bankroll luxury homes, fancy cars, expensive clothes and jewelry, and nights spent in clubs and casinos. When law enforcement was about to swoop in and arrest the thief, he managed to flee the country and continue his extravagant lifestyle abroad for about four years.

Eventually, thanks to investigators who wouldn't give up and international partners who provided vital support, this man was found and returned to the U.S. to face justice. Last month, Tobechi Onwuhara, of Dallas, Texas—the ringleader of a multi-million-dollar fraud scheme and a former FBI wanted cyber fugitive—was sentenced to federal prison. Seven additional co-conspirators have either pled guilty or been convicted.

There's no shortage of schemes that identity thieves perpetrate to line their own pockets—from stealing credit card numbers and fraudulently applying for loans and refunds to breaking into online bank accounts. Onwuhara's specialty? He targeted home equity line of credit accounts, a form of revolving credit in which your home serves as collateral.

How the scheme worked: Onwuhara and his co-conspirators identified potential victims—people who had home equity line of credit accounts with large balances—by accessing certain fee-based websites often used in the real estate industry for customer leads (one of Onwuhara's associates was a real estate agent). After collecting bits of personally identifiable information from those websites—like names, addresses, dates of birth, and Social Security numbers—and then using other online sites to obtain personal information to help with passwords and security questions, they were able to access victims' credit reports online, which contained loan balances and other financial and personal information.

Armed with this information, Onwuhara would either call a customer service representative at a victim's financial institution while impersonating the victim—or gain access to the victim's online account—and request a transfer of funds from the home equity line of credit account into the victim's checking or savings account. From those accounts, he'd request that the money be wired to another bank account—usually overseas and always one that he controlled.

To help with the impersonation, Onwuhara would use caller ID spoofing services to display the customer's legitimate phone number. And in case the financial institution needed to call the customer back for some reason before the money was wired, Onwuhara—again impersonating the victim—would call the victim's telephone company and request call forwarding to another phone (which of course belonged to a member of his criminal group).

Once the money was transferred, Onwuhara paid money mules in several different countries to withdraw the money and get it back to Onwuhara's criminal enterprise.

Our investigation of Onwuhara's scheme—which involved hundreds of victims nationwide, attempts to steal more than $38 million, and losses of $13 million—began in late 2007 after we received a complaint from a Washington, D.C.-area victim. We were ultimately able to identify and gather evidence against Onwuhara and his crew, and federal charges were handed down in August 2008. After he fled the U.S., ongoing international law enforcement efforts continued until December 2012, when he was located in Sydney, arrested by the Australian National Police, and returned to this country.

A Byte Out of History

The Five-Decade Fugitive Chase

Frank Grigware was serving a life sentence for robbing a mail train in Nebraska when he escaped from the United States Penitentiary in Leavenworth in 1910, and a young Bureau was handed one of its first investigations. It turned out to be one of the longest-running cases in our history.

USP Leavenworth, the nation's first federal penitentiary, was still under construction in Kansas on that April morning when Grigware and five other convicts made their escape—carving a piece of wood into the shape of a revolver to dupe the guards and busting through the prison gates in a hijacked locomotive used to haul supplies and new inmates into the complex.

Within hours, four of the fugitives were captured. A few days later, the fifth man was found. Only Grigware remained missing. The Bureau of Investigation—the forerunner of today's FBI—was notified. For years, agents pursued numerous leads across the country and around the world. Grigware was reportedly spotted masquerading as everything from a Catholic priest to a traveling salesman. Catching the now-fabled fugitive became something of a national obsession.

In reality, Grigware had fled to Canada, eventually settling in northern Alberta under the name James Fahey. He began a new life, running a confectionery store, building homes, and becoming active in his church. In 1915, he moved to the small town of Spirit River and was elected mayor the next year. Along the way, he married and had a family.

During those years, the Bureau's investigation ebbed and flowed as leads dried up and larger events—like World War I—took over. In 1928, the case was reignited, and the following year, the Bureau learned of a credible sighting of Grigware in Edmonton more than a decade earlier. The fugitive's photo and fingerprints were sent to the Royal Canadian Mounted Police (RCMP). By 1933, however, after no success, the Bureau closed its case. Still, a standing wanted notice was kept in place.

Three months later, nearly a quarter century after Grigware's prison break, the mystery was finally solved. After Grigware was caught poaching in Canada, he was fingerprinted by local authorities. His prints were sent to the RCMP, where an astute clerk matched them to the set sent years before by the Bureau.

A wanted poster was issued for Frank Grigware after he escaped from federal prison in 1910.

The story doesn't end there, though. The Canadian press suggested that Grigware was innocent of the original charges (which may well have been true) or that he deserved mercy. Many Canadians agreed. They flooded Ottawa and Washington with petitions urging that Grigware be allowed to remain in Canada. In 1934, the U.S. dropped its extradition request.

But could Grigware return to the U.S. to visit his family, his niece asked in 1957? The Department of Justice ruled against this since he had never been officially pardoned, so the FBI kept tabs on Grigware until formally closing the case in 1965. Grigware died in 1977 at the age of 91.

In the end, the pursuit of the former mayor of Spirit River lasted more than a half century. Though Grigware was hardly a dangerous fugitive, the case shows how the keys to the Bureau's success were already coming into focus in its early years: the tireless quest for justice, the mix of old-fashioned investigative legwork with modern scientific principles like fingerprinting, and the formation of solid partnerships with colleagues across borders. It's only fitting that one of the FBI's first cases would end up incorporating so many features of our modern-day investigations.

Botnet Bust

SpyEye Malware Mastermind Pleads Guilty

Today, Russian national Aleksandr Andreevich Panin pled guilty in an Atlanta federal courtroom to a conspiracy charge associated with his role as the primary developer and distributor of malware—called SpyEye—created specifically to facilitate online theft from financial institutions, many of them in the U.S.

SpyEye infected more than 1.4 million computers—many located in the U.S.—obtaining victims' financial and personally identifiable information stored on those computers and using it to transfer money out of victims' bank accounts and into accounts controlled by criminals.

Ultimately, though, Panin sold his malware online to the wrong customer—an undercover FBI employee. And after an investigation involving international law enforcement partners as well as private sector partners, a dangerous cyber threat was neutralized.

How the conspiracy operated. From 2009 to 2011, Panin conspired with others, including co-defendant Hamza Bendelladj (charged and extradited to the U.S. last year), to advertise and develop various versions of SpyEye in online criminal forums. One ad described the malware as a "bank Trojan with form grabbing possibility," meaning it was designed to steal bank information from a web browser while a user was conducting online banking. Another ad said that the malware included a "cc grabber," which scans stolen victim data for credit card information.

Panin sold the SpyEye malware to more than 150 "clients" who paid anywhere from $1,000 to $8,500 for various versions of it. Once in their hands, these cyber criminals used the malware for their own nefarious purposes—infecting victim computers and creating botnets (armies of hijacked computers) that collected large amounts of financial and personal information and sent it back to servers under the control of the criminals. They were then able to hack into bank accounts, withdraw stolen funds, create bogus credit cards, etc.

In February 2011, a search warrant allowed the FBI to seize a key SpyEye server located in Georgia. It was several months after that when the FBI bought SpyEye online from Panin—which turned out to be very incriminating because that particular version contained the full suite of features designed to steal confidential financial information, make fraudulent online banking transactions, install keystroke loggers, and initiate distributed denial of service (DDoS) attacks from computers infected with malware.

Panin was arrested in July 2013 while he was flying through Hartsfield-Jackson Atlanta International Airport.

The investigation into the SpyEye malware is just one initiative worked under Operation Clean Slate, a broad public/private effort recently undertaken to eliminate the most significant botnets affecting U.S. interests by targeting the criminal coders who create them and other key individuals who provide their criminal services to anyone who'll pay for them. Much like the FBI's other investigative priorities where we focus on taking down the leaders of a criminal enterprise or terrorist organization, under Clean Slate we're going after the major cyber players who make botnets possible.

And FBI Executive Assistant Director Rick McFeely warns potential hackers: "The next person you peddle your malware to could be an FBI undercover employee… so regardless of where you live, we will use all the tools in our toolbox—including undercover operations and extraditions—to hold cyber criminals accountable for profiting illicitly from U.S. computer users."

A Byte Out of History

$10 Million Hack, 1994-Style

It was hardly the opening salvo in a new era of virtual crime, but it was certainly a shot across the bow.

Two decades ago, a group of enterprising criminals on multiple continents—led by a young computer programmer in St. Petersburg, Russia—hacked into the electronic systems of a major U.S. bank and secretly started stealing money. No mask, no note, no gun—this was bank robbery for the technological age.

Our case began in July 1994, when several corporate bank customers discovered that a total of $400,000 was missing from their accounts. Once bank officials realized the problem, they immediately contacted the FBI. Hackers had apparently targeted the institution's cash management computer system—which allowed corporate clients to move funds from their own accounts into other banks around the world. The criminals gained access by exploiting the telecommunications network and compromising valid user IDs and passwords.

Working with the bank, we began monitoring the accounts for more illegal transfers. We eventually identified approximately 40 illegal transactions from late June through October, mostly going to overseas bank accounts and ultimately adding up to more than $10 million. Meanwhile, the bank was able to get the overseas accounts frozen so no additional money could be withdrawn.

The only location where money was actually transferred within the U.S. was San Francisco. Investigators pinpointed the bank accounts there and identified the owners as a Russian couple who had previously lived in the country. When the wife flew into San Francisco and attempted to withdraw funds from one of the accounts, the FBI arrested her and, soon after, her husband. Both cooperated in the investigation, telling us that the hacking operation was based inside a St. Petersburg computer firm and that they were working for a Russian named Vladimir Levin.

We teamed up with Russian authorities—who provided outstanding cooperation just days after a new FBI legal attaché office had been opened in Moscow—to gather evidence against Levin, including proof that he was accessing the bank's computer from his own laptop. We also worked with other law enforcement partners to arrest two co-conspirators attempting to withdraw cash

from overseas accounts; both were Russian nationals who had been recruited as couriers and paid to take the stolen funds that had been transferred to their personal accounts.

In March 1995, Levin was lured to London, where he was arrested and later extradited back to the United States. He pled guilty in January 1998.

Believed to be the first online bank robbery, the virtual theft and ensuing investigation were a needed walk-up call for the financial industry…and for law enforcement. The victim bank put corrective measures in place to shore up its network security. Though the hack didn't involve the Internet, the case did generate media coverage that got the attention of web security experts. The FBI, for its part, began expanding its cyber crime capabilities and global footprint, steadily building an arsenal of tools and techniques that help us lead the national effort to investigative high-tech crimes today.

Four MS-13 Leaders Sentenced

Serious Threat Removed from Atlanta Streets

For nearly four years, four leaders of various Mara Salvatrucha, or MS-13, factions operating in the Atlanta metro area terrorized the community through their flagrant disregard for life—conspiring to commit senseless acts of murder, attempted murder, and armed robbery.

But a multi-year, multi-agency law enforcement effort recently took down this criminal enterprise, eradicating a deadly threat from the streets of Atlanta. Ernesto Escobar, Miguel Alvarado-Linares, and Dimas Alfaro-Granados will be spending the rest of their lives in prison, while Jairo Reyna-Ozuna will be behind bars for more than a decade.

The MS-13 gang is composed primarily of immigrants and/or their descendants from El Salvador, Guatemala, and Honduras. In the U.S., this extremely violent criminal organization got its start in Los Angeles and then spread out to a number of states around the country, including Georgia.

In Atlanta, as in other areas, members are usually organized into groups called "cliques" that operate under the larger MS-13 umbrella. Each clique has a leader who conducts regular meetings to plan and discuss crimes against rival gangs. In this case, we saw clique leaders reporting back to MS-13 leaders in their home countries about MS-13 activities in the Atlanta area.

The four defendants in this case, who reportedly lived by the credo "rape, kill, control," perpetrated their crimes for seemingly minor reasons—to enhance their reputations among fellow gang members, to protect their turf from rival gangs, or to exact revenge for a real or perceived slight. The robberies were usually committed to obtain funding to support the criminal enterprise, providing money and weapons to gang members—including incarcerated individuals in the U.S. and elsewhere.

Some of the heinous crimes the defendants were charged with included:

- Murdering a fellow MS-13 member who was thought to be cooperating with police;
- Ordering an MS-13 member who wanted to leave the gang to first commit an act of violence, leading the departing member to shoot into a car believed to be carrying rival gang members—killing the passenger and wounding the driver;
- Returning to a nightclub following a fight with a suspected rival gang member and fatally shooting a man walking through the club's parking lot;
- Going back to a gas station after a scuffle with two teenagers who worked there and fatally shooting one of them as he painted lines in the parking lot; and
- Murdering a 15-year-old boy—a suspected 18th Street gang member—with a shotgun.

The case was investigated by the Atlanta Safe Streets Task Force, made up of investigators from local, state, and federal agencies, including the FBI. Another key partner was the U.S. Immigration and Customs Enforcement's Homeland Security Investigations Directorate.

Federal participation in this case allowed a number of effective tools to be brought to the table—perhaps most importantly the RICO (Racketeer Influenced and Corrupt Organizations) and the VICAR (Violent Crimes in Aid of Racketeering) statutes with their tougher penalties. Investigators also made use of physical and court-authorized electronic surveillances and confidential informants.

The charges against the four subjects in this case were part of a broader multi-agency investigation of MS-13 in Atlanta, concluded in 2010, which resulted in arrests of, charges against, and/or deportation of 75 members.

Proof positive that dedicated, cooperative efforts among law enforcement agencies can and do win out over dangerous criminal conspiracies.

Serial Killers

Part 5: Wayne Williams and the Atlanta Child Murders

On July 21, 1979, a 14-year-old boy disappeared. Four days later, another teen went missing. Both, it was soon learned, had been killed.

It was the beginning of a shocking series of murders—some 29 in all—that would take place over the next 22 months in Atlanta. The victims were all young African-Americans, and as the death toll mounted, so did fear and tension across the city.

The FBI's involvement in the case began on June 22, 1980 following the abduction of a 7-year-old girl. The Atlanta Police Department, which—along with the Georgia Bureau of Investigation—was investigating the string of killings, asked the FBI if the federal kidnapping statute had been violated.

None of the crimes appeared to fall under federal law, but Special Agent in Charge John Glover—the first African-American to lead an FBI field office—offered all the support the Bureau could give under the circumstances. Our Atlanta office helped follow up on out-of-state leads. The FBI Lab provided assistance. And our Behavioral Sciences Unit sent an expert to develop a profile of a possible perpetrator.

Meanwhile, the murders continued. Local politicians, the news media, and even Georgia Senator Sam Nunn asked the Department of Justice to permit FBI involvement, and the attorney general did so on November 6, 1980, authorizing a preliminary investigation. On November 17, the Bureau launched a major case investigation, devoting more than two dozen agents and other personnel to the case full time.

FBI agents joined local and state law enforcement officers on a task force investigating the murders. Collectively, they focused on a dozen disappearances with several shared traits. The victims were all young African-American males who vanished in broad daylight in fairly public locations. Their bodies were found in desolate areas. Their murders had no obvious motivation (in contrast, two other homicides from that period appeared to have been gang-related). These commonalities suggested a single killer.

The case continued through the winter and into the spring of 1981. By late April, however, the killer began to change his behavior, dumping the victims' bodies in the Chattahoochee River. Members of the task force staked out the 14 bridges in the Atlanta metropolitan area that crossed the river and patiently waited.


TO: DIRECTOR, FBI
(Attn: Latent Fingerprint Section, Section Supervisor [redacted])
FROM: SAC, ATLANTA (7A-1835) (P)
SUBJECT: [redacted]
ATKIDS;
MAJOR CASE #30
KIDNAPING
OO: ATLANTA
Re telcal to SA [redacted]
Enclosed for the Identific
separate cover are sixty-eight (68)
major case prints of Wayne Bertram W
fingerprints and palm prints of Nath
REQUEST OF THE LATENT FINGERPRINT SECTION
Compare submitted latent prints with enclosed prints of Williams and Cater, as well as all available prints of victims.

Evidence linked Wayne Williams, inset above over one of the files in his case, to 22 murders in Atlanta beginning in 1979. The FBI's involvement began in 1980 following the abduction of a 7-year-old girl.

On May 22, a big break came in the case. One of the groups conducting surveillance—consisting of an FBI agent, an Atlanta police officer, and two police cadets—heard a loud splash around 2:52 a.m. A car sped across the bridge, turned around in a parking lot on the other side, and sped back across the bridge. The vehicle was pursued and stopped. The driver was a 23-year-old African-American freelance photographer named Wayne Williams.

Lacking probable cause, authorities let Williams go. But when the body of a young African-American man named Nathaniel Cater was found downstream two days later, more attention was paid to Williams. Investigators soon learned that his alibi was poor and that he had been arrested earlier that year for impersonating a police officer. Later, he failed multiple polygraph examinations.

Williams was arrested on June 21, 1981. He was convicted of two murders on February 27, 1982, after he was linked to the victims through meticulous hair and fiber analysis and witness testimony. Following the trial, the law enforcement task force concluded that there was enough evidence to link Williams to another 20 of the 29 deaths. He went to jail for life, and the Atlanta child killings stopped.

Part 6: Andrew Cunanan Murders a Fashion Icon (page 21)

Protecting Aircraft from Lasers

New Program Offers Rewards for Information

Today the FBI announced a program aimed at deterring people from pointing lasers at aircraft—a felony punishable by five years in jail—and rewarding those who come forward with information about individuals who engage in this dangerous activity.

"Aiming a laser pointer at an aircraft is a serious matter and a violation of federal law," said Ron Hosko, assistant director of the FBI's Criminal Investigative Division. "It is important that people understand that this is a criminal act with potentially deadly repercussions."

The new initiative—which includes a campaign to educate the public about the dangers of "lasing"—will run for 60 days in 12 FBI field offices where laser strikes against aircraft are prevalent. A key part of the program is reward money: The Bureau will offer up to $10,000 for information leading to the arrest of any individual who intentionally aims a laser at an aircraft.

"Laser pointers are legal and certainly have legitimate uses," said George Johnson, a federal air marshal who serves as a liaison officer with the Bureau on laser issues. "Used in the wrong environment, however, they can be very dangerous."

When aimed at an aircraft from the ground, the powerful beam of light from a handheld laser can travel more than a mile and illuminate a cockpit, disorienting and temporarily blinding pilots. Those who have been subject to such attacks have described them as the equivalent of a camera flash going off in a pitch black car at night.

Since the FBI and the Federal Aviation Administration (FAA) began tracking laser strikes in 2005, there has been a more than 1,000 percent increase in the number of incidents with these devices, which can be purchased in stores or online for as little as a few dollars. Last year, 3,960 laser strikes against aircraft were reported—an average of almost 11 incidents per day. And it's estimated that thousands of attacks go unreported every year.

"We hope that more public awareness about this issue will lower the instances of laser strikes," Johnson said. "We also want to encourage people to come forward when they see someone committing this felony—one that could have terrible consequences for pilots and their passengers." As of December 2013, the FAA had documented at least 35 incidents where pilots required medical attention after a laser strike.

Interfering with the operation of an aircraft has long been a federal crime, but the FAA Modernization and Reform Act of 2012 specifically made it a federal felony to knowingly point the beam of a laser at an aircraft. The new law lowered the threshold for prosecution, Johnson said, "and the trend is on the rise for jail time in these cases." Last month, for example, a 23-year-old California man was sentenced to 21 months in prison for aiming a laser pointer at a Fresno County Sheriff's Office helicopter. Court records showed that the man deliberately tracked and struck the aircraft.

The 12 FBI offices participating in the new program are Albuquerque, Chicago, Cleveland, Houston, Los Angeles, New York City, Philadelphia, Phoenix, Sacramento, San Antonio, San Juan, and the Washington Field Office.

If you have information about a lasing incident or see someone pointing a laser at an aircraft, call your local FBI office or dial 911.

The Gangs of Los Angeles

Part 1: Innovative Approaches to a Serious Problem

At 5 a.m., the command post in our Los Angeles Division was buzzing with activity. It would be a day of reckoning for nearly two dozen members of MS-13, the violent street gang that over the years has brought drugs, murder, and misery to countless Los Angeles neighborhoods.

Before the sun came up, teams of FBI agents and their partners from the Los Angeles Police Department (LAPD) began making arrests. In short order, the large video monitors in the command post started to show the words "in custody" next to the images of the subjects—many of whom were wanted on federal drug charges and were the gang's leaders, or "shot callers," in the parlance of the street.

In Los Angeles—often referred to as the gang capital of the world—it was just another day for the men and women of the FBI who work to protect the community from hundreds of area gangs. But locking up these criminals is only part of the story. Together with our law enforcement and community partners, the Los Angeles Division is taking a leadership role in the fight against gangs with innovative programs designed to bring healing as well as justice to neighborhoods ravaged by violence and intimidation.

"You can't arrest your way out of the gang problem," explained Robert Clark, an assistant special agent in charge in our Los Angeles Division. "Looking at the statistics prior to 2007 and in the seven years since I've been here," he said, "there's been upwards of a 300 percent increase in arrests, but the gang problem still exists."

Clark and others considered new approaches. "Where could we bring our resources and our like ideas to really have an impact in the community?" he asked. "FBI agents and local police officers can't be everywhere. That's why it was important that we build relationships in the community. Those relationships are essential to solving crimes."

Understanding firsthand the challenges facing gang-plagued neighborhoods based on his own childhood growing up in the inner city of Youngstown, Ohio,

Through the FBI's Community Impact Initiative, law enforcement personnel and other volunteers return to neighborhoods after gang busts to clean alleyways, working alongside residents and property owners.

Clark spearheaded three initiatives that are making a difference in Los Angeles. In the coming weeks, FBI.gov will chronicle those programs, which are helping to empower communities, reduce the crime rate, clear unsolved murder cases, and aid in intelligence-gathering efforts that allow the Bureau to monitor gangs with an international reach such as MS-13.

The programs include:

- Operation Save Our Streets Task Force, established in 2010 in partnership with the LAPD to solve gang-related homicide cases;
- The Community Impact Initiative, in which law enforcement personnel and other volunteers return to neighborhoods after gang busts to clean alleyways of trash and graffiti, working alongside residents and property owners; and
- The Homicide Library project, a joint initiative between the FBI and the LAPD that is digitizing thousands of paper-only murder investigation files for use in a searchable system that will help solve more cases.

"Thanks to the hard work of many, many people," Clark said, "we have been able to take these ideas and implement them and measure their success. We have been able to take murderers off the streets," he added, "and just as importantly, we are helping to improve the quality of life in communities where residents often felt forgotten or ignored."

Part 2: Operation Save Our Streets (page 14)

The Gangs of Los Angeles

Part 2: Operation Save Our Streets

The murders may be random and senseless—a drive-by shooting that kills an innocent bystander—or they may be targeted hits by individuals "putting in work" against rival gang members. Either way, officials estimate that more than half of all the homicides that occur in Los Angeles are gang related.

To address the problem, the FBI joined with the Los Angeles Police Department (LAPD) in establishing a gang homicide task force in 2010 called Save Our Streets (SOS). It was an idea born of necessity, and it has been extremely successful.

"We've had a record number of homicide clearances because of the SOS effort," said FBI Los Angeles Assistant Special Agent in Charge Robert Clark. The task force—which Clark proposed—focuses on murder investigations that are close to being solved but need an extra investigative push and other resources to result in indictments and arrests.

"Recognizing that there were a large number of unsolved gang-related homicides in L.A., we decided to pool our resources," Clark said, "and have seasoned FBI investigators and LAPD homicide detectives work together to solve cases."

"The FBI offered us everything from personnel to laptops," said Cheryl Nalls, an LAPD detective who works in the Criminal Gang/Homicide Division in South Central L.A. "We have a serious gang problem here,"

Left: FBI task force members conduct an operation in Los Angeles.

she said, adding that in 2010, lack of funds threatened to imperil many gang-related homicide investigations.

In that year, a city budget crisis forced administrators to place a cap on the amount of overtime homicide detectives could work, which meant that some investigations were put at risk. The SOS initiative provided temporary federal funding to pay overtime costs along with investigative manpower and additional resources.

During the initial 90-day trial period of SOS in 2010, 27 homicide cases were cleared, a number that was "unheard of in such a short period of time," Clark said. The following year, during the same 90-day period from July through September, SOS task force officers cleared 50 homicide cases.

"A host of things are being done in L.A. to contribute to the annual murder rate dropping to record lows," Clark said, "and SOS is absolutely a part of that. We've cleared more than 200 cases since the program began, and that means we've sent more than 200 people to jail. SOS puts murderers behind bars."

Today, the SOS Task Force has become a permanent part of the FBI's anti-gang operations in Los Angeles, and Clark is able to assign task force officers to the city's gang hotspots.

Special Agent Bob Scheerle, an SOS member, currently sits with his LAPD counterparts in the police department's Harbor office in southern Los Angeles—a jurisdiction where there are seven major gangs, methamphetamine is the illicit drug of choice, and the majority of murders are gang-related.

Having agents and detectives sitting together, working cases side by side, makes for a true partnership, Scheerle said, "and that helps solve more cases."

"Those relationships are what make SOS work, not just funding and equipment," Clark added. "We are all working toward a common goal—to make the community a better place in which to live."

Nalls agrees. "SOS has been a win-win for everybody," she said, "but most especially for the community."

Part 3: Helping to Heal Communities (page 15)

The Gangs of Los Angeles

Part 3: Helping to Heal Communities

Driving along the streets and alleyways of Baldwin Village—known as "The Jungle" and historically one of the most violent gang neighborhoods in South Central Los Angeles—homicide detective Cedric Washington can recall in detail the many gang-related shootings and murders he has investigated there. In his 17 years with the Los Angeles Police Department, he has learned a hard truth: "It's too easy to become a victim here."

But Washington also sees something else in Baldwin Village. Beyond the violence and the victims, he sees a restored neighborhood taking shape. Part of the credit for that goes to an FBI program he helped establish. It's called the Community Impact Initiative, and it's designed to work *after* law enforcement puts gang members behind bars.

The program brings together law enforcement personnel and volunteers from a variety of government, business, and community organizations to work alongside residents and property owners to clean up alleyways, paint over graffiti, and install security cameras—all to help residents stake a new claim on their neighborhoods.

"A few years ago, we were arresting dozens of gang members at a time," said Robert Clark, an assistant special agent in charge in our Los Angeles Division. "That was impactful, but then someone said: 'You arrested X number of gang members. How did that improve the quality of life in that particular neighborhood?'" The question, he remembered, "caught us flat-footed, because for law enforcement, it usually stops at the numbers—the arrest statistics. We realized there was more that we could do."

Clark, Washington, and others organized the first community impact day after a major gang takedown in Baldwin Village and enlisted more than 100 volunteers to donate time and materials. "The city has existing programs to mitigate trash and graffiti," Clark said, "so we partnered with them as well."

The result of that and a second cleanup effort was that "children were able to return to the playground," Clark said, "and people could walk to the shopping areas and feel safe."

Los Angeles Police Department Detective Cedric Washington discusses the Community Impact Initiative as FBI Los Angeles Assistant Special Agent in Charge Robert Clark (far left) and other partners look on.

With gang members in jail, the crime rate went down—and stayed down. "Because of our law enforcement action and the community impact piece," Clark said, "we've been able to maintain a double digit reduction in the crime rate in Baldwin Village."

The Community Impact Initiative has now become a regular part of the Bureau's anti-gang operations. "After the bad guys have been arrested and removed," Clark said, "we roll back into those communities within 90 days with our volunteers."

That causes residents to view law enforcement in a different way. "Some folks think all we do is arrest people," Clark said. "A lot of people in these neighborhoods feel ignored and forgotten. But then they see us working with them to improve where they live."

The Community Impact Initiative works because it builds relationships, Clark explained. "We have breakfast with residents and face-to-face conversations. They see that we care about their quality of life." In return, residents are more willing to cooperate with law enforcement, which helps solve cases and adds to the reduction in crime.

"I've seen generations of young kids in these neighborhoods with such potential," Washington said. "Then you fast forward and they're in gangs. But because of our enforcement efforts and the community impact days, Baldwin Village is getting better," the detective said. And that gives him hope. "I can see the results of our efforts."

Part 4: The Homicide Library (page 18)

A (Driver's) License to Steal

Corruption in a San Diego Motor Vehicle Office

You could call this scam a license to steal, and it certainly was—until it all came crashing down on the corrupt state employees and their accomplices who were selling California driver's licenses for cash.

For at least three years, though, between 2009 and 2012, the scammers had a nearly seamless operation that netted a tidy profit. Here's how it worked:

A man who owned a driving school let his students know that—for a price—he could guarantee them a license, even if they had already failed the driving test. Often they didn't even have to take the test, thanks to the man's connections at the Department of Motor Vehicles (DMV) office in El Cajon, California.

Those willing to pay anywhere from $500 to $2,500 to corrupt DMV employees could get a license with no questions asked. The driving school catered mostly to Middle Eastern immigrants, and soon word of easy licenses in that community spread north to Los Angeles and beyond.

"One guy flew in from Dallas, took a cab to the DMV office, paid for his license, and flew back to Dallas a few hours later," said Special Agent Mike Peters, who investigated the case with Special Agent Kim George out of our San Diego Division. "It was so blatant," Peters said, "that our surveillance showed the driving school operator brokering multiple deals in the DMV parking lot."

"They had gotten away with it for so long," added George, "that they were extremely confident and had no plans to stop."

Court records indicate that the group—which included Kuvan Piomari, who owned the U.S. Driving School in El Cajon; Jeffrey Bednarek, a DMV examiner who conducted driving tests; and three other DMV employees—took part in the long-running bribery conspiracy that produced hundreds of ill-gotten licenses.

In exchange for bribes, Bednarek falsely entered passing scores for written and behind-the-wheel tests for applicants seeking regular and commercial driver's licenses. He enlisted other DMV employees to falsify records as well. Bednarek produced more than 100 fraudulent driver's permits, for which applicants paid a total of more than $50,000.

Sometimes the corrupt DMV employees would issue multiple bogus licenses a day, George said. "They would leave work with $500 in cash in their pocket. That could be one day a week or two. They were doing very well."

When a new manager arrived at the El Cajon DMV office, however, "she instantly realized that something wasn't right," Peters said. The new manager alerted the DMV's investigative arm, who in turn called the FBI.

Using undercover operatives and court-authorized surveillance and wiretaps, investigators quickly uncovered the scam. Some of the "candidates" who paid for licenses were bad drivers, George explained, "and some paid because they were just too lazy to take the test."

Peters added that some candidates had paid for commercial licenses that allowed them to drive tanker trucks. "That took things to a different level in terms of public safety," he said.

In all, 30 defendants have been charged with conspiracy to commit bribery and identification document fraud, and all have pled guilty. The case is ongoing. Bednarek is scheduled to be sentenced in April. Another DMV employee, Jim Bean, was sentenced to 18 months in prison for his role in the scheme.

"We hope this case sends a message," Peters said. "This type of corruption will not be tolerated."

Historic Insider Trading Scheme

Stock Manager Busted

For Mathew Martoma, 2008 seemed like a banner year. As an up-and-coming portfolio manager for the hedge fund company SAC Capital, he helped earn $275 million in profits and avoided losses related to trades involving pharmaceutical companies and an experimental Alzheimer's drug. He even took home a $9 million bonus in the process.

If that sounds too good to be true—especially during a rocky year for the stock market—that's because it was. Martoma's success was based not on his investment savvy but on illegally obtained inside information. Earlier this month, he was convicted of securities fraud in a Manhattan federal court in what U.S. Attorney Preet Bharara called "the most lucrative insider trader scheme ever charged."

Martoma went to work for SAC Capital in 2006 and was responsible for investment decisions related to public companies in the health care sector. At the time, two pharmaceutical companies were involved in clinical trials for a new Alzheimer's drug. One of Martoma's first steps was to reach out to expert networking firms—businesses that arrange paid consultations between financial industry clients and experts in various fields who can offer advice, analysis, and market research. This was all perfectly legal, since the information exchanged wasn't considered material, non-public data.

But Martoma wanted more. Through an expert networking firm, he connected with two doctors involved in the Alzheimer's drug trials who he knew would have the kind of confidential information he wanted.

From 2006 until July 2008, Martoma arranged for dozens of "consultations" with these doctors, often engaging in subterfuge to disguise the nature of their communications (e.g., sending e-mails to schedule meetings or phone calls on bogus topics). Taking full advantage of his financial and personal relationships with them, Martoma managed to solicit inside information on the drug trials that led him and SAC Capital to trade aggressively…racking up millions in profits.

Early on, information from one of the doctors included generally positive safety data about the drug. After receiving that information, Martoma purchased shares

of both pharmaceutical companies' stock for his portfolio and recommended that SAC Capital do the same across the board. By spring 2008, SAC Capital held approximately $700 million worth of stock in these two companies.

But in mid-July 2008, one of the doctors—who later became a cooperating witness and testified against Martoma at his trial—discovered some unsettling information about the new drug: Alzheimer's symptoms in patients taking the drug had consistently gotten worse over time. Chosen to make a public announcement about these drug trial results at an international Alzheimer's conference on July 29, 2008, the doctor quickly forwarded the information to Martoma. And just as quickly, Martoma and SAC Capital unloaded nearly all of their stock in the two companies—thus avoiding huge losses when the announcement about the drug trial results became known.

The case began in 2009, when our partners at the Securities and Exchange Commission referred to us incidents of suspicious trading in two health care stocks by SAC Capital. After reviewing trading records and other documentation, we identified Martoma. And subsequent investigative efforts—which included executing search warrants, reviewing financial and other business records, interviewing witnesses, and reviewing e-mail evidence—culminated in Martoma's arrest in December 2012.

Through this investigation and many others like it, we continue to work against corruption in U.S. financial markets to help ensure fairness in the marketplace.

Left: Boxes containing "murder books"—binders filled with information on homicide investigations—are stacked at a Los Angeles Police Department facility. The FBI is helping to digitize these files for use in a fully searchable homicide library.

The Gangs of Los Angeles

Part 4: The Homicide Library

In a room at a Los Angeles Police Department (LAPD) facility, thick binders—most filled with more than a thousand pages of paper—are stacked in boxes on and under tables and piled from floor to ceiling. Each binder represents a murder victim.

Dubbed "murder books" by the LAPD, they hold the contents of individual homicide investigations, from witness statements and crime scene photos to autopsy reports. The FBI is helping to turn these paper-only books into a digital homicide library that will benefit investigators as well as the families of victims.

The project will take nearly 5,000 murder books going back to 1990 and digitize them for use in a system that will be fully searchable so that LAPD detectives—as well as FBI analysts and investigators—will be able to cross-reference and compare information in every case, something not currently possible.

"Not only will this help solve cases," said LAPD Det. Cheryl Nalls, who is administering the project, "it will bring healing to the families of victims."

Over the years, the LAPD developed a system where all paper material related to a homicide investigation is put into a binder. Each murder book has tabs where particular information is placed. That way, any detective inheriting a case understands how the paperwork is organized.

"The system works," Nalls said, "but because it is paper only, the material in the binders is only useful to the investigator on that case. Potential leads involving other cases, victims, or subjects are locked inside the book."

And when a homicide case is officially inactive for one year, it goes dormant and the murder book is placed into one of several retention files located at various locations within the LAPD's 21 geographical areas. The result is that hundreds of unsolved cases could potentially end up filed away and forgotten.

"The homicide library will change all that," said Robert Clark, an assistant special agent in charge in our Los Angeles Division who worked with LAPD Capt. Nancy Lauer to launch the digital library idea. "Being able to search and cross-reference 20 years of homicide data on solved and unsolved cases is something that has never existed."

Murder books are shipped to the FBI's Document Conversion Lab in Virginia, where each record in every book is scanned into a software system that allows for sophisticated searching and archiving. The Bureau will maintain the digital network.

"We are essentially digitizing the investigative process," Clark said, which has intelligence value for the Bureau as well as the LAPD. Agents working other federal investigations or analysts looking for gang and murder trends, for example, will be able to use the system to add and extract information.

The LAPD has committed funds to create and maintain a physical space for the homicide library, where the murder books will be stored and made available to victims' families. They will be able to visit the library to find out the status of loved ones' cases, and perhaps offer new information that could help solve a case.

"We want to bring healing to families," Nalls said.

About 1,000 books have been scanned and uploaded so far. Beta testing is underway, and Nalls says she hopes the system will be operational by the end of 2014. The homicide library project has been "a great innovation," she said, "and a great partnership between the LAPD and the FBI."

Part 5: The Power of Partners and Intelligence (page 20)

Naval Espionage

Stopping a Dangerous Insider Threat

As a sailor with a top secret clearance, a sensitive job on a submarine, and 20 years of service in the Navy, Robert Hoffman possessed a tremendous amount of knowledge about the U.S. nuclear fleet and its operations—knowledge he was willing to sell to the Russians.

"It's almost impossible to say why someone would become a spy," said Special Agent James Dougherty, who investigated the case from our Norfolk Division, but Hoffman represents a classic example of the insider threat. "When a U.S. citizen with classified information threatens to betray his country," Dougherty explained, "the resulting damage to national security and loss of American lives can be catastrophic."

Investigators speculate that Hoffman may have blamed his divorce on the Navy, along with his failure to gain promotion. The FBI and the Naval Criminal Investigative Service (NCIS) became concerned in 2011 when, nearing retirement, Hoffman told friends he was going on a "man-cation" to Belarus to see Russian women he had previously met when he was stationed in Bahrain—even though he knew the women would not be there.

"He had some sort of motivation to travel to Belarus that didn't seem logical," said Dougherty. In addition, Hoffman ignored the requirement to alert military security officers that he would be traveling out of the country, and he failed to adhere to other security rules of reporting any suspicious incidents while overseas. However, Hoffman did post items on social media channels saying he met the president of Belarus. "All of that added to our suspicion," Dougherty noted.

Using court-authorized surveillance, wiretaps, and other investigative tools, FBI and NCIS investigators began monitoring Hoffman's movements at his home in Virginia Beach following his retirement from the Navy in late 2011. Soon after, our undercover operatives made contact with him to assess his intentions.

Then, in September 2012, a female FBI undercover agent posing as a Russian operative knocked on Hoffman's door and delivered a message ostensibly from Russian intelligence officials.

"He received instructions from the woman, who asked him to respond by e-mail within one week," Dougherty said. "We didn't want to pressure him. We wanted him to make a conscious decision, knowing he would be dealing with the Russian intelligence service."

The encrypted thumb drive containing top secret national defense information that Robert Hoffman gave to what he thought was the Russian intelligence service.

Hoffman didn't wait a week—he responded within hours. He agreed to answer a series of questions on an encrypted thumb drive that was to be left in a hollow tree in a park—a hiding place known in the spy world as a dead drop. On the third such drop, Hoffman divulged top secret national defense information.

"American lives could have been lost based on the information he was willing to give up," Dougherty said. "He had access to things that were highly, highly sensitive."

In August 2013, a jury in Norfolk found Hoffman guilty of attempted espionage; last month, the 40-year-old was sentenced to 30 years in prison.

"The insider threat is very real," said Dougherty, explaining that in these types of cases, there are often people who are suspicious of a friend or colleague's statements or behavior but who don't act on those suspicions.

"One of the things we teach in insider threat training," Dougherty said, "is that if you see something, say something. Often, people don't want to rock the boat," he added, "but if you see something that doesn't seem right, it's your legal obligation to report it. Let the FBI sort it out. That's what we get paid for."

The Gangs of Los Angeles

Part 5: The Power of Partners and Intelligence

In Los Angeles and the sprawling metropolitan area that surrounds the city, there are approximately 800 different gangs, each of them engaged in various levels of violence and criminal activity.

"There was a time when we talked about gangs in terms of individuals standing on street corners selling rocks of crack cocaine," said Robert Clark, an assistant special agent in charge in our Los Angeles Division who supervises the Bureau's gang program there. "But the threat has evolved," he said. "We now have gangs that are involved in regional, national, and international criminal enterprises."

There are still open-air drug markets in certain neighborhoods, Clark explained, but the gangs have grown more sophisticated, branching out to extortion, money laundering, identity theft, and human trafficking. All of that can exact a heavy toll on the community.

To counter the threat, the FBI partners with local and state law enforcement organizations and numerous federal agencies. Through a variety of task forces and intelligence platforms, the goal is to leverage all of law enforcement's resources to dismantle the worst gangs from the top down.

"The most significant threats that impact the communities—the shootings, murders, and robberies—are easy to see," Clark said. "But we also look at the entire criminal enterprise, the infrastructure that allows gangs to control neighborhoods and extort and intimidate people who live there."

Left: FBI Los Angeles Assistant Special Agent in Charge Robert Clark walks through a trash-strewn alleyway in a gang-plagued neighborhood. The FBI partners with multiple agencies on a variety of initiatives designed to dismantle gangs as well as help communities.

Intelligence gathering and sharing is critical to law enforcement's success, Clark noted. "And good intelligence happens when you have strong partnerships." The Bureau's international gang investigations may be helped by intelligence gleaned from a local gang case. "We may be able to recruit new sources or open new investigations based on what we learn locally," he said.

And the information flows both ways. The Los Angeles City Attorney's office, for example, is able to fight the gang threat through a unique initiative that benefits from its partnership with the FBI.

"Traditionally," said Jonathan Cristall, a supervising city attorney who runs the Federal and Local Special Abatement Operations Program, "prosecutors deal with problem people. Our program targets problem places that serve as bases of operations for the gangs and negatively impact public safety."

The city attorney's office obtains injunctions requiring property owners to implement improvements to properties. They can also obtain court orders that prohibit gang members from setting foot back in the neighborhood. "If they come back," Cristall added, "they can be arrested on sight."

In the civil courts, the city attorney often moves against gang members and the properties they control on the same day the FBI makes criminal arrests. That requires close coordination—and the Bureau's willingness to share sensitive information about its operations. "Today, we work with many of the federal law enforcement agencies," Cristall said. "But one of the first agencies to bring us on board as a trusted partner was the FBI."

He added that when his office first started this type of work, "there were so many spots in L.A. where the gangsters felt like they owned that neighborhood. Those areas are harder to find now," said Cristall.

Clark sees the abatement program as one more tool in law enforcement's fight against gangs. "Collectively, when we apply all of our resources," he said, "we can bring justice to the people in communities hard hit by gangs."

Part 6: Working to Make a Difference (page 31)

Serial Killers

Part 6: Andrew Cunanan Murders a Fashion Icon

Around 8:45 on the morning of July 15, 1997, international fashion designer Gianni Versace returned home to his Miami Beach mansion on Ocean Drive following a walk to a local café.

Suddenly, a man approached Versace, pulled out a pistol, and killed him with two shots to the back of his head. The man fled—followed at a distance by at least one witness—and disappeared into a nearby parking garage.

Miami Beach homicide detectives soon asked for assistance from the FBI's local field office in the city. The officers were concerned that the killing might be a murder-for-hire, but evidence quickly suggested that it wasn't. Inside the parking garage identified by the witness was a red pickup truck linked to a murder in New Jersey and a man named Andrew Phillip Cunanan, the target of an ongoing manhunt.

Cunanan was a 27-year-old college dropout from California. He was highly intelligent, spoke two languages, and since his teenage years had sought to live a life of riches and comfort. He had supplemented his earnings from an odd job here and there by serving as a male prostitute and engaging in longer-term liaisons with older homosexuals who would shower him with gifts and cash.

For reasons that remain unclear, Cunanan had begun a murderous spree in late April 1997. First, he bludgeoned a former naval officer to death with a hammer in Minneapolis. A few days later, he shot and killed an architect and dumped his body near East Rush Lake in Minnesota. Both men were his long-time associates. In May, Cunanan targeted a stranger—a 72-year-old real estate developer—in Chicago. Cunanan stole the man's car, and, less than a week later, murdered a cemetery worker in New Jersey. He then took that victim's red truck and drove to Miami.

Throughout this time, authorities were putting together the pieces. The investigation and forensic work linked the Chicago murder and the others to Cunanan. On May 7, the FBI joined the search for Cunanan and quickly marshaled its resources to identify and interview his friends, family, and other contacts. The New Jersey murder made it clear Cunanan was moving across the country, and gay groups were especially concerned that he might insinuate himself into their circles and continue to commit murders. The New York City Gay and Lesbian Anti-Violence Project posted a large reward and sought to warn those who might know Cunanan.

Murderer Andrew Cunanan was added to the FBI's Ten Most Wanted Fugitives list on June 12, 1997, shortly before he killed Gianni Versace.

Working with the television show *America's Most Wanted*, the FBI made Cunanan the 449th addition to its Ten Most Wanted Fugitives list on June 12, 1997. Our offices in Minnesota, California, Illinois, New Jersey, and elsewhere continued to seek information about him. The Bureau also publicized a telephone tip line and disseminated details on the FBI's public website. But Cunanan slipped under the radar.

With the murder of Gianni Versace, though, the net began to close. Eight days later, on July 23, 1997, the caretaker of a houseboat about two miles north of Versace's house in Miami Beach reported hearing a gunshot. Responders found Cunanan dead from a self-inflicted wound. His killing spree was over.

Part 7: The FBI and Jeffrey Dahmer (page 61)

Investigating Tax Refund Fraud

FBI Works Cooperatively with Federal Partners

A Georgia woman was recently sentenced to 27 years in prison for stealing the identities of nursing home patients and using their information to apply online for about half a million dollars in fraudulent tax refunds from the Internal Revenue Service (IRS).

Criminals who use stolen personally identifiable information to line their own pockets perpetrate a wide variety of fraudulent financial schemes, like hacking into online accounts, submitting phony insurance claims, and applying for loans and credit cards. Increasingly, though, tax refund fraud using stolen identities is fast becoming a favorite money-making endeavor of the criminal element.

The IRS has reported a significant increase in identity theft-related tax refund fraud over the past several years. This type of crime is perceived by criminals and organized criminal enterprises as relatively easy, seemingly low-risk, and, ultimately, pure profit which can be used to fund other criminal activities—like drug trafficking, money laundering, public corruption, or even terrorism.

Anyone with a Social Security number could become a victim. But criminals who commit tax refund fraud seem to focus more on people who don't normally file tax returns—the elderly, low-income families, students, patients at long-term health care facilities, and even the homeless. Perpetrators also target public figures like celebrities, athletes, CEOs, and politicians, as well as law enforcement, military, and government personnel—including Attorney General Eric Holder.

How a scheme works. The perpetrator fills out a federal tax return online with stolen identity information and phony wage and tax withholding figures, then informs the IRS how to provide the refund (a check mailed to a certain address, a direct deposit into a bank account he controls, or, more common these days, a deposit onto a debit card in his possession).

In simple tax refund schemes, one person usually handles everything—from obtaining stolen identities to collecting refunds. But in more sophisticated schemes, there are a number of individuals assuming different roles: "ringleaders" who organize entire operations, "sources" who steal identity information, "preparers" who file returns online, and "runners" who actually collect the proceeds.

Law enforcement response. The dedicated work done by IRS-Criminal Investigation professionals is a major component of that agency's efforts to combat tax-related identity theft. And the IRS continues to make enhancements in fraud prevention, early detection, and victim assistance as well.

But the FBI—working with our partners at the IRS and U.S. Secret Service and through liaison efforts with banks—brings valuable investigative resources to the table: our years of experience investigating financial crimes, our focus on identifying and dismantling large criminal networks, and our use of sophisticated investigative techniques. We also share intelligence and information with other federal law enforcement partners to help link investigations of criminal organizations engaged in tax fraud schemes that may be tied to illegal drugs, weapons, terrorism, or other types of criminal activity.

All of these efforts are paying off—we've been part of many successful cases recently.

And the FBI will continue to work cooperatively to investigate stolen identity tax refund fraud—we take our role in identifying and arresting those responsible very seriously. These crimes not only victimize law-abiding individuals but all honest U.S. taxpayers who ultimately foot the bill for this stolen revenue.

Help Us Find a Killer

American Contractor Murdered in Iraq in 2009

American contractor James Kitterman was last seen alive on the evening of May 21, 2009, in Baghdad, Iraq. His body was found the next day inside his vehicle, and his killer or killers are still at large.

Although nearly five years have passed since Kitterman's death, the FBI investigation continues. Today we are announcing a reward of up to $20,000 for information leading to the identification, arrest, and conviction of the person or persons responsible for the murder.

"We have put a lot of effort into this case," said Special Agent Marc Hess, who is leading the investigation from our Washington Field Office. "We have interviewed more than 100 potential witnesses in Iraq, Afghanistan, the U.S., and the Philippines—but despite our efforts, we need the public's help."

A poster seeking information has been placed on our website and is available in Arabic and Tagalog in addition to English. Anyone with information about the case is encouraged to contact their local FBI office or the nearest American Embassy or Consulate, or to submit a tip online. All tips can remain anonymous.

Kitterman, who was 60 at the time of his death, owned a private construction company and was contracted by the U.S. government to build a helipad at the U.S. Consulate in Baghdad. The work was taking place inside the Green Zone—the roughly four-square-mile area housing U.S. military personnel and their international coalition partners located in central Baghdad. Kitterman lived and worked inside the Green Zone, which was considered a secure area for Americans and had security provided by locally recruited guards.

Complicating the investigation is that possible witnesses—as well as suspects—are scattered around the world. During that time period, contractors came to work in Iraq from many countries. Kitterman's now-defunct company, Peregrine Eyes, recruited its employees from various countries, although the majority of the workers were from the U.S. and the Philippines.

Hess, who has been working the Kitterman case since 2010, has coordinated with the FBI's legal attaché offices to help enlist the support of our international law

enforcement colleagues. He believes the $20,000 reward may help bring more people forward, particularly in Iraq.

"Although the international aspect of this case has made it difficult," Hess added, "what's important is what is always important in investigations—that people who have information need to come forward and do the right thing."

Since the murder, Hess has been in regular contact with Kitterman's brother. "The family isn't giving up on finding his killer," Hess said, "and neither is the FBI." He added that Kitterman was well liked and respected in the international contracting community, "and his employees all said he treated them like family."

Help us locate those responsible for James Kitterman's murder. "He deserves justice," Hess noted, "and his killer or killers deserve to be caught and held accountable."

Note: The suspect(s) in this case may have been located since the above information was posted on our website. Please check our Seeking Information webpage at www.fbi.gov/wanted/seeking-info for up-to-date information.

The *Exxon Valdez*, 25 Years After

FBI Continues to Support Environmental Crime Enforcement Partners

On March 24, 1989—25 years ago today—the massive oil tanker *Exxon Valdez* ran aground on Bligh Reef in Alaska's Prince William Sound. The ship was outbound from Port Valdez and carried 53 million gallons of crude oil; an estimated 11 million gallons spilled into the Gulf of Alaska.

The harm caused by the spill was extensive. Tens of thousands of animals died, generations of fish and other marine life were compromised, the lives of residents were greatly disrupted, and the ongoing effects of this catastrophe continue today. Clean-up costs were astronomical.

Particularly since the 1970s amid growing concerns about the environment, a series of federal laws have been added to the government's authority to investigate abuses of our shared environment, looking for criminal activity that threatens lives and health. In the case of the *Exxon Valdez*—and in most environmental crime cases at the time—the FBI worked closely with state and other federal agencies to determine what happened, how it happened, and if criminally negligent behavior was involved.

In February 1990, after an extensive investigation into the incident, the Department of Justice brought a multi-count criminal indictment against Exxon Corporation and its shipping subsidiary for violations of the Clean Water Act, the Refuse Act, and the Migratory Bird Treaty Act (this particular law had been part of the FBI's jurisdiction

Left: The *Exxon Valdez* is seen following its devastating 1989 oil spill in Alaska. (NOAA Photo)

since the 1920s), among others. And in October 1991, the U.S. District Court in Anchorage accepted guilty pleas by Exxon and approved a settlement involving a criminal plea agreement and restitution. Exxon paid a hefty fine; however, a portion of it was returned due to the company's support of clean-up efforts. The court also approved a civil settlement resolving claims with the federal government and Alaska for clean-up costs and damage to natural resources—the civil penalties were even higher than the criminal fines.

Fast Forward: The FBI's Role Today

In 2014, with the Bureau's overriding focus on preventing terrorist attacks—along with efforts to address cyber crimes and emerging national security and criminal threats—our environmental role is largely a supporting one, assisting our partners at the Environmental Protection Agency, the Coast Guard, and state and local agencies.

But our focus on criminal activity that threatens lives remains the same. Working with other agencies, the FBI generally focuses on significant environmental crime cases in the following areas:

- **Knowing endangerment**, where the crime puts people in danger;
- **Catastrophic events**, like huge oil spills or explosions;
- **Patterned flagrant violators**, which include companies that shrug off their fines;
- **Government abuse and public corruption**, because the government has to obey the laws, too; and
- **Organized crime**, which often involves waste and illegal dumping.

The Bureau brings unique tools to the investigative table—including sophisticated techniques like court-authorized electronic surveillance, undercover operations, and informants—that we've used successfully for years against organized crime groups, drug traffickers, financial crime fraudsters, and the like. And we continue to assist our partners in bringing the most egregious violators to justice.

For information on the Department of Justice's overall efforts to go after abusers of the nation's civil and criminal pollution-control laws, visit its Environmental and Natural Resources Division website.

New Top Ten Fugitive

MS-13 Member Wanted for Double Murder

Juan Elias Garcia, wanted for the execution-style murder of a 19-year-old New York woman and her 2-year-old son, has been named to the Ten Most Wanted Fugitives list.

A reward of up to $100,000 is being offered for information leading directly to the arrest of Garcia, who is alleged to be a member of the violent Mara Salvatrucha gang—MS-13—and may be hiding in El Salvador.

"Garcia's callous disregard for human life resulted in the senseless murder of a young mother and her helpless 2-year-old son," said George Venizelos, assistant director in charge of our New York Field Office. "His appointment to the FBI's Top Ten list illustrates not only the seriousness of his crimes but our commitment to seeking justice for his victims."

The murders occurred in Central Islip, New York in 2010. At that time, Garcia—who is known by the nickname "Cruzito"—was 17 years old.

"MS-13 is the most violent gang here of any of the street gangs," said Special Agent Reynaldo Tariche, who investigated the case with other members of the FBI's Long Island Gang Task Force. While gang-related murders are not uncommon on Long Island, "the execution of a 2-year-old and his mother is a new low even for MS-13," Tariche noted.

Garcia had a romantic relationship with the 19-year-old victim, Vanessa Argueta, who had ties to the 18th Street gang and the Latin Kings, two of MS-13's rivals. After a falling out between Argueta and Garcia, rival gang members allegedly threatened Garcia. When he relayed that information to fellow MS-13 members—that he had been threatened because of information provided by Argueta—it was decided to retaliate against her.

"They were going to kill her for disrespecting the gang," said Special Agent James Lopez, also a member of the task force. According to gang code, Lopez explained, "it is unacceptable for MS-13 members to have girls they associate with be involved with rival gang members."

"Garcia was an enthusiastic murderer," Tariche said. "He was the reason why this happened. He was the one who decided to get the gang involved. It wasn't about a boyfriend-girlfriend dispute. This was about disrespecting the gang. And the penalty for that is death."

On February 4, 2010, Garcia invited Argueta to dinner but instead lured her and her son into the woods. Along with two other MS-13 members, he executed her with two shots from a handgun while her son looked on. The gun was then turned on the child. The first shot knocked him to the ground but did not kill him. The boy got up and clutched at Garcia's leg, but another gang member shot again and killed him

Garcia should be considered armed and dangerous. He is 5 feet 4 inches tall, weighs 125 pounds, and has black hair and brown eyes. He is known to speak Spanish and English and has ties to Santa Rosa de Lima in El Salvador as well as Nicaragua, Honduras, Guatemala, and Panama. His two co-conspirators have been convicted of murder and are awaiting sentencing. A fourth defendant charged in connection with the murders—Garcia's MS-13 leader—has been sentenced to three terms of life in prison, plus 60 years.

We need your help: If you have any information concerning the whereabouts of Juan Elias Garcia, contact the FBI's New York Field Office or your nearest law enforcement agency or U.S. Embassy or Consulate. You can also submit a tip online.

Note: Juan Elias Garcia surrendered to authorities at the U.S. Embassy in Managua, Nicaragua on March 27, 2014.

Child Predator

Help Us Identify John Doe 28

The FBI is seeking the public's help to stop a child predator.

The unidentified individual we are seeking is known only as John Doe 28. In November 2012, online video of the man engaging in sexually explicit activities with a young boy was reported to the National Center for Missing & Exploited Children (NCMEC), an organization that works closely with the Bureau to stop child predators.

The video contains a brief image of the alleged predator, which investigators hope will lead to his identification—and the recovery of the exploited child. "Subjects who show their faces in child pornography are not typical," said Special Agent Karen Jurden. "It is our hope that someone will recognize this individual and come forward. We were able to recover a very clear image of John Doe 28."

Working with NCMEC, investigators in our Violent Crimes Against Children program have enhanced other details from the video that could be clues to help identify the suspect. For example, the video shows the individual and the victim inside a residence with what appears to be a blue chair and a picture hanging on a wall in the background. Someone familiar with the house might easily recognize the chair. Also, John Doe 28 is wearing wire-framed glasses and a burgundy T-shirt with a fish logo on it.

There are no details linking the suspect to a particular area, but Jurden said investigators believe he may be a U.S. citizen because he speaks one word during the video—"careful"—which is in English.

"Sometimes we will get some type of identifier that narrows down the geographic region," said Jurden, who has been investigating crimes against children for the last four years, "but that didn't happen in this case. That's why we are asking for the public's help nationwide."

Left: The child predator known as John Doe 28 is seen in stills pulled from a video.

The video is just over two minutes long and was recovered during the arrest of a San Francisco man on child pornography charges. "The video was part of his collection," Jurden added, explaining that sexually explicit videos and images of children are often traded anonymously through online forums.

The efforts to identify and apprehend John Doe 28 are part of the FBI's Operation Rescue Me and Endangered Child Alert Program (ECAP) initiatives and represent a longstanding partnership with NCMEC. Operation Rescue Me identifies child victims of sexual exploitation by using sophisticated image analysis to obtain evidence. ECAP seeks public and media assistance to help identify the John and Jane Does who display their faces—and other distinguishing characteristics such as tattoos—in pornographic images and videos of children.

Since the inception of ECAP in 2004, 28 John/Jane Does have been investigated; 20 of these cases have been successfully resolved so far. These investigations have led to the identification of nearly 70 child victims.

We need your help. John Doe 28 appears to be a Caucasian male in his 30s or 40s who has a receding hairline and wears wire-framed glasses. Anyone with information should submit a tip online or call the FBI's toll-free tip line at 1-800-CALL-FBI.

"We need to identify John Doe 28," Jurden said, "so we can make sure no harm comes to that little boy."

Note: John Doe 28 may have been located since the above information was posted on our website. Please check our ECAP webpage at www.fbi.gov/wanted/ecap for up-to-date information.

FBI Honors Community Leaders

Their Efforts to Improve Lives Lauded

The FBI and law enforcement agencies around the country diligently work for the good of the communities we serve and for the nation as a whole. But we can't do it alone—we also need the support of the people who live in those communities.

Today, at FBI Headquarters in Washington, D.C., we publicly recognized 58 individuals and organizations from communities around the country for giving us that support. The recipients of our annual Director's Community Leadership Award have made tremendous contributions toward crime and violence prevention, education and awareness programs, and efforts to enhance cooperation between law enforcement and all citizens.

Addressing the award winners during the ceremony, Director James Comey said, "You are the truly extraordinary among us .... You see injustice in your communities and you take action—showing a true willingness to lead when others may choose to walk away."

We present these awards publicly—first at the local FBI field office and then at this yearly national ceremony—with the hopes that others will hear the stories of the recipients and be inspired to create change in their own communities and help make their neighborhoods safer.

Here are just a few of those inspiring stories:

- An Albuquerque civil rights advocate—whose goal is to convince people to be "change agents" in their communities—continues his four decades of work toward building coalitions to improve the lives of all Americans, regardless of race.
- A former law enforcement officer-turned-community activist in Atlanta uses the game of chess to reach disadvantaged youth by teaching them the practical skills and techniques needed to overcome life's obstacles.
- A Delaware social services agency focuses on meeting the needs of the state's growing Latino population through programs dedicated to the healthy development and education of children, youth, and their families.

- After the unsolved murder of her 14-year-old daughter, a Cleveland mother now assists other parents who have lost children to violence and creates educational opportunities for underprivileged youth.
- A non-profit organization in Las Vegas helps southern Nevada's homeless and at-risk veterans and their families with rapid re-housing, employment assistance, training, and other services.
- A Louisville cardiologist and civic leader—a voice for the local Muslim community—coordinates meetings and public service projects between Muslim, Christian, and Jewish leaders with the aim of reducing stereotypes within the community.
- A survivor of human trafficking and advocate for human trafficking victims dedicates her efforts in Milwaukee to ensuring adequate resources for victims and educating young people and adults on the issues of sexual violence, sexual exploitation, and sex trafficking.
- A Seattle man facilitates stronger ties between members of the Seattle-area Somali community and local and federal law enforcement by hosting numerous gatherings and fostering an environment of understanding and dialogue.

Congratulations to each of our award recipients for going above and beyond the call to service…for reaching out to those in need…and for supporting law enforcement's efforts to better our communities—and our nation.

Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/dcla2013.

Helping Victims and Their Families

Psychologist Specializes in Kidnapping, Hostage Cases

A U.S. aid worker is kidnapped for ransom in Somalia. A terrorist group holds an American hostage in Afghanistan. Sometimes incidents like these make headlines, and sometimes they occur below the media radar. Either way, the FBI's Office for Victim Assistance (OVA) is there to help victims and their families.

When the FBI investigates crimes, federal law requires that we offer assistance and services to victims. In situations where Americans are taken hostage overseas, our go-to person in the OVA is an operational psychologist with decades of real-world experience.

Carl Dickens joined the Bureau in 2011 after a 32-year career in the military in which he spent more than 13 years in special operations and personnel recovery and deployed multiple times in support of combat operations. His insights and practical knowledge help investigators working to recover victims, and also help victims—and their families—resume their lives.

"My job starts the moment a person goes missing," Dickens explained. "The FBI uses an integrative approach to hostage cases that not only supports individuals and their families but also synchronizes the investigative and operational elements working to get the person back."

When the FBI is alerted to an overseas hostage situation, Dickens and his colleagues in the OVA's Terrorism and Special Jurisdiction Program coordinate with other FBI

Left: Carl Dickens joined the FBI in 2011 after a 32-year career in the military.

units and federal partners involved in the effort to recover the individual. The OVA will also locate the victim's family and dispatch a victim specialist there for support (the Bureau has victim specialists in all 56 of its field offices).

"Families of kidnap victims are dealing with one of the most stressful events in their lives," Dickens said. "Unfortunately there are no roadmaps for a family when something like this happens," he added. "While their loved one is being held, we try to offer families a sense of hope. We let them know there are people actively working to recover their family member and that we aren't giving up." In addition to providing emotional support, the OVA team can assist with travel, lodging, and emergency expenses and can provide notification about criminal proceedings.

Dickens understands how a hostage might react to the stresses of captivity, which can be helpful to those planning a rescue operation or preparing for the victim's safe return home. He can also help to assess the hostage's coping response and develop a post-captivity support plan for the individual's return.

Kathryn Turman, who leads the OVA, noted that the FBI has been increasingly called on to handle overseas hostage cases. "We knew we needed someone like Carl, and we were incredibly fortunate that he joined the FBI," she said. "His practical knowledge helps investigators, and his efforts with recovered victims and their families make a significant difference in how well they are able to cope and move forward in their lives."

Experience has taught Dickens that most hostages find an inner strength when they are in captivity. "Recovered victims are not broken or damaged," he said. "They are just normal people who have gone through an abnormal situation. It's important for families to recognize that their loved one may be weak and shaken when they come home," he explained, "but they are not broken."

Helping victims and families find the way forward is "a noble profession," he added. "To see the look on the face of someone who has been recovered, and to know that you were part of that effort, is very gratifying."

New Top Ten Fugitive

'Family Annihilator' William Bradford Bishop, Jr. Wanted for 1976 Murders

William Bradford Bishop, Jr., wanted for the brutal murders of his wife, mother, and three sons in Maryland nearly four decades ago, has been named to the Ten Most Wanted Fugitives list.

A reward of up to $100,000 is being offered for information leading directly to the arrest of Bishop, a highly intelligent former U.S. Department of State employee who investigators believe may be hiding in plain sight.

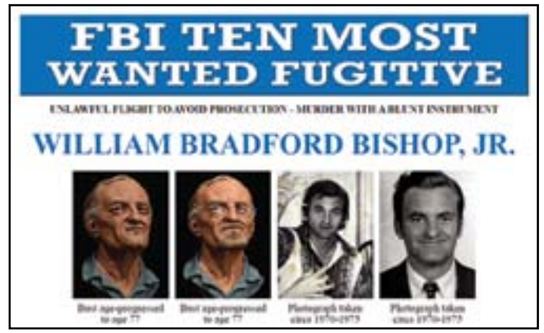
On March 1, 1976, Bishop used a hammer to bludgeon his family, including his three boys, ages 5, 10, and 14. Investigators believe he then drove to North Carolina with the bodies in the family station wagon, buried them in a shallow grave, and set them on fire. The last confirmed sighting of Bishop was one day after the murders at a sporting goods store in Jacksonville, North Carolina, where he bought a pair of sneakers.

"Nothing has changed since March 2, 1976 when Bishop was last seen except the passage of time," said Steve Vogt, special agent in charge of our Baltimore Division. Vogt has teamed with local Maryland law enforcement officials to apprehend Bishop, a man described by investigators as a "family annihilator."

"There is no indication that Bishop is dead," Vogt said, explaining that the area where the bodies were discovered was searched extensively, and hundreds of individuals were interviewed at the park where the abandoned station wagon was later discovered—there was no trace of Bishop.

The FBI, the Montgomery County Police Department, the Montgomery County Sheriff's Office, and the Department of State formed a task force last year to take another look at the Bishop case and to engage the public in locating him. As part of that effort, a forensic artist created a three-dimensional, age-enhanced bust of what the fugitive may look like now, at the age of 77.

Naming Bishop to the Top Ten list is expected to bring national and international attention to the case in a way that was impossible decades ago. "When Bishop took off in 1976, there was no social media, no



24-hour news cycle," Vogt said. "There was no sustained way to get his face out there like there is today. And the only way to catch this guy is through the public."

"If Bishop is alive—and there is every chance that he could be," said Tom Manger, chief of the Montgomery County Police Department and a member of the task force, "we are hopeful someone will call with the tip we need to catch him." Manger added, "When you have a crime of this magnitude, no matter how long ago it occurred, the police department and the community never stop trying to bring the person responsible to justice."

"No lead or tip is insignificant," Vogt explained. "If Bishop is living with a new identity, he's got to be somebody's next-door neighbor." Vogt, a Maryland native who remembers when the murders happened 38 years ago, echoed Manger's sentiments about never giving up trying to locate the fugitive. "Don't forget that five people were murdered," he said. "Bishop needs to be held accountable for that."

We need your help: If you have any information concerning William Bradford Bishop, Jr., contact your local FBI office, the nearest law enforcement agency, or the appropriate U.S. Embassy or Consulate. You can also submit a tip online.

Note: William Braford Bishop, Jr. may have been located since the above information was posted on our website. Please check our Ten Most Wanted Fugitives webpage at www.fbi.gov/wanted/topten for up-to-date information.

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

Advice for U.S. College Students Abroad

Be Aware of Foreign Intelligence Threat

Three years ago, Glenn Duffie Shriver, a Michigan resident and former college student who had studied in the People's Republic of China (PRC), was sentenced to federal prison in the U.S. for attempting to provide national defense information to PRC intelligence officers.

According to the Institute of International Education, more than 280,000 American students studied abroad last year. These experiences provide students with cultural opportunities and can equip them with technical and leadership skills that make them marketable to U.S. private industry and government employers.

But this same marketability makes these students tempting and vulnerable targets for recruitment by foreign intelligence officers whose long-term goal is to gain access to sensitive or classified U.S. information. Glenn Shriver—prodded by foreign intelligence officers into eventually applying for U.S. government jobs—cited his naivety as a key factor in his actions.

The FBI has ramped up efforts to educate American university students preparing to study abroad about the dangers of knowingly or unknowingly getting caught up in espionage activities. As part of these efforts, we're making available on this website our *Game of Pawns: The Glenn Duffie Shriver Story* video, which dramatizes the incremental steps taken by intelligence officers to recruit Shriver and convince him to apply for jobs with the U.S. State Department and the Central Intelligence Agency. We'd like American students traveling overseas to view this video before leaving the U.S. so they're able to recognize when they're being targeted and/or recruited.

Left: Glenn Duffie Shriver describes his experience being recruited by PRC intelligence officers.

How do foreign intelligence officers routinely interact with students?

- Foreign intelligence officers don't normally say they work for intelligence services when developing relationships with students—they claim other lines of work.
- Intelligence officers develop initial relationships with students under seemingly innocuous pretexts such as job or internship opportunities, paid paper-writing engagements, language exchanges, and cultural immersion programs.
- As relationships are developed, the student might be asked to perform a task and provide information—not necessarily sensitive or classified—in exchange for payment or other rewards, but these demands grow over time.
- Intelligence officers might suggest that students—upon completion of their schooling—apply for U.S. government jobs (particularly for national security-related agencies).

What can students do to protect themselves while studying abroad?

- Be skeptical of "money-for-nothing" offers and other opportunities that seem too good to be true, and be cautious of being offered free favors, especially those involving government processes such as obtaining visas, residence permits, and work papers.
- Minimize personal information you reveal about yourself, especially through social media.
- Minimize your contact with people who have questionable government affiliations or who you suspect might be engaged in criminal activity.
- Properly report any money or compensation you received while abroad on tax forms and other financial disclosure documents to ensure compliance with U.S. laws.

And when you return to the U.S., report any suspicious activity to your local FBI office. You can also contact your local U.S. Embassy or Consulate while abroad.

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

The Gangs of Los Angeles

Part 6: Working to Make a Difference

When Special Agent Robert Clark speaks to an inner city school group or residents who live in Los Angeles neighborhoods overrun by gangs, he doesn't think of himself as an outsider.

"I don't see myself as separate from a lot of the people that I meet in the community," said Clark, an assistant special agent in charge in our Los Angeles Division who supervises the Bureau's gang operations there. "I see myself as one of them, because I used to be one of them. I grew up in the inner city. I grew up in foster care. I grew up in places where violence was commonplace, and gangs, graffiti, and drugs were everywhere."

For that reason, Clark is committed to dismantling violent gangs through rigorous law enforcement efforts. He is equally committed to helping young people avoid the gang life and empowering residents to take back their neighborhoods. Since coming to Los Angeles seven years ago, he has spearheaded several gang initiatives with community, civic, and law enforcement partners that go beyond merely arresting gang members and sending them to jail.

"I can relate so much to what these kids go through and the violence that they see," Clark explained. "I was involved in some of that as a youngster, but I realized very early that it was not for me. Thankfully, I had some teachers that believed in me and made sure I stayed on the straight and narrow. They made sure that my life mattered."

Growing up in a gritty section of Youngstown, Ohio, known then for its connections to organized crime, Clark's life could have gone either way. "My father was a nightclub owner," he said. "He worked for the mob and ran nightclubs for the mob—girls, numbers, drugs, that whole life. That's what my father did. He was murdered when I was 12 years old. I was the last one to see him alive."

A college scholarship to play football got Clark out of Youngstown; after college, he became a police officer and eventually joined the FBI. "I knew that my life had to count," he said. "The impact my childhood had on me—

FBI Los Angeles Assistant Special Agent in Charge Robert Clark discusses efforts to tackle the gang problem.

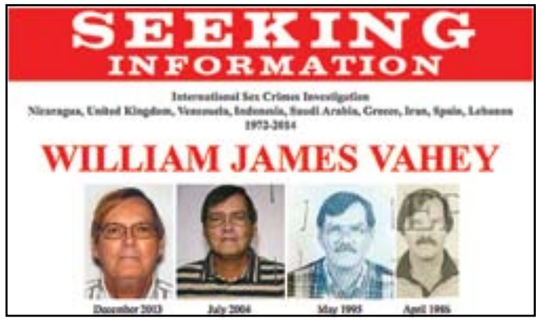
how I grew up and the things that I was able to escape from—made me want to give something back."

He is now in a unique position to do just that.

"I recognize that I can influence young people in gang neighborhoods," Clark noted. "Most of these kids have never seen an FBI agent, much less an African-American FBI agent. When they see me, I want to stand as an example and tell them, 'You, too, can come from this environment and still succeed if you go to school and work hard. It doesn't matter what your situation is at home. It doesn't matter if mom or dad is not there, or dad's in prison, or whatever the case may be. You can achieve something.'"

"Robert takes great pride in his work and helping communities to heal and become whole," said Cheryl Nalls, a Los Angeles Police Department detective who has worked closely with Clark in some of the worst gang neighborhoods in South Central L.A. "He is a passionate advocate," she added, "and it's important for people in these communities to see someone like that."

"I come to work every day to make a difference," Clark said.



Seeking Information

International Child Exploitation Case

The FBI is asking for the public's help to identify victims of a suspected serial child predator who taught in private American schools overseas in nine different countries beginning in 1972 and whose young victims—believed to be boys between the ages of 12 and 14—may be unaware of what happened to them.

William James Vahey, a 64-year-old U.S. citizen who was jailed in California in 1969 for child molestation, committed suicide last month days after his employer saw a thumb drive belonging to him that contained pornographic images of boys who were likely drugged. At the time, Vahey was teaching ninth-grade world history and geography at the American Nicaraguan School in Managua.

When confronted about the images by a school administrator, Vahey confessed that he was molested as a child and had preyed on boys his entire life, giving them sleeping pills prior to the molestation.

The thumb drive contained sexually graphic images of at least 90 victims, according to Special Agent Patrick Fransen. The photographs were cataloged with dates and locations that corresponded to Vahey's overnight field trips with students beginning in 2008. However, the investigation has revealed that Vahey accompanied students on similar trips throughout his career.

Fransen, a 16-year FBI veteran who specializes in crimes against children, noted that Vahey had been teaching at American schools overseas since the 1970s. "I'm concerned that he may have preyed on many other students prior to 2008," he said. "I've never seen another case where an individual may have molested this many children over such a long period of time."

At this point in the investigation, photographed victims are being identified and notified. Those who believe they may have been victims are being encouraged to come forward—not only to aid investigators but potentially to seek services through our Office for Victim Assistance. A confidential questionnaire is available for anyone who thinks they may have been victimized by Vahey or who may have information about his predatory behavior.

In addition to teaching, Vahey coached boys' basketball teams at several of the schools where he taught. The popular and highly respected teacher regularly organized overnight field trips and coordinated itineraries that included boys' room assignments.

"He had access to children because of his position of trust," Fransen said. "He created a system that gave him the opportunity and the means to molest children. The manner in which he committed these acts—while the boys were unconscious—may have inhibited them from knowing what happened, making it impossible for them to come forward at the time of the molestation."

By his own admission, Vahey used sleeping pills to drug his victims, but investigators want to learn more about his methods and what drugs he may have used. They are hopeful the public can assist them.

Vahey traveled extensively over the past four decades, teaching at American schools in Nicaragua, the United Kingdom, Venezuela, Indonesia, Saudi Arabia, Greece, Iran, Spain, and Lebanon. His victims are multinational. In addition to foreign nationals, the schools were attended by the children of American diplomats, military personnel stationed overseas, and other American citizens working abroad.

As the investigation unfolds, the FBI continues to work with our international partners in the affected countries through our legal attaché offices and the U.S. Department of State. "At this time, investigators have no knowledge that Vahey shared or traded any of the pornographic material he made," Fransen said. "But his suicide left a lot more questions unanswered than answered."

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

Investment Fraud Scheme Uncovered

Members of Military and Dependents Victimized

They are our nation's heroes—often risking their lives abroad to protect us at home. Which makes what one Virginia con man did all the more despicable…defrauding military personnel and their dependents in an investment fraud scheme.

But one of his victims came forward and filed a complaint. And after a joint investigation conducted by the Richmond offices of the FBI and the U.S. Postal Inspection Service (USPIS)—under the auspices of the Virginia Financial and Securities Fraud Task Force—Vernon Matthews was charged in the scheme, pled guilty, and was recently sentenced to a federal prison term.

Matthews operated a company called First Capital Group (FCG), located in Virginia Beach. He had a license to sell insurance, not to give investment advice or handle securities—but that didn't stop him from doing so. Starting in 2010 and continuing until early 2013, Matthews solicited members of the military and their families to make investments with FCG.

Often times, he set up booths at establishments known to be frequented by the military—like restaurants located near military bases—and offered promotions, like a free night at a hotel. And when potential victims came to his office to claim the prizes, Matthews would pitch them on an investment.

And he lied through his teeth while doing it. Among Matthews' misrepresentations:

- He received compensation from the U.S. government for his investment advice and services (he did not);
- He would invest his clients' funds in certificates of deposits, mutual funds, or something similar (Matthews misappropriated all the funds for his own personal or business use);
- FCG was affiliated with several reputable investment companies and funds (it was not);
- The investment provided a good return—anywhere from 4 to 300 percent—and was low-risk or no-risk (it did not and was not).

In one particular instance, a U.S. Naval Academy graduate who invested $20,000 with FCG tried withdrawing funds. Matthews mailed a check that bounced. After being notified about it, he mailed another one…and instructed the victim not to deposit the check until he could put the funds into his account. That, of course, never happened.

Matthews received more than $235,600 from victim investors. Only a few of his victims were able to recover any money, so at his sentencing, the judge ordered Matthews to repay the outstanding balance of $204,465 in restitution to his victims.

The Bureau joined the investigation in April 2013. In July 2013—after an extensive review of financial records, documents, and e-mails, along with interviews of dozens of victims and other witnesses—Matthews was arrested.

The Virginia Financial and Securities Fraud Task Force was initially launched in 2010 to establish a partnership between criminal investigators—including the FBI and the USPIS—and civil regulators to investigate and prosecute complex financial fraud cases in Virginia. The state task force is also an investigative arm of the national Financial Fraud Enforcement Task Force, an interagency group created to wage an aggressive, coordinated, and proactive effort to investigate and prosecute financial crimes.

And while law enforcement, civil regulators, and prosecutors are doing all they can to address financial crimes, you should educate yourself and your loved ones on how to avoid becoming a victim of financial fraud.

Understanding School Impersonation Fraud

A Look Inside the Scam

The operator at the office supply store call center answers the phone, and the person on the other end claims to be a school purchasing officer with questions about his account. But the caller is actually a criminal, and the information the operator may unwittingly divulge could cost the retailer hundreds of thousands of dollars.

It's called the school impersonation scheme, and it has been carried out in nine states across the country—mostly by Nigerian criminal groups using the Internet and social engineering techniques.

"Most retailers have been pretty good about catching the scam," said Special Agent Alla Lipetsker, "but it's an alarming trend, and the fraudsters have had success."

Here's how the scam works:

- A member of the criminal group poses as a school official on the telephone or by e-mail and uses social engineering—actions that deceive individuals into revealing otherwise secure information—to learn about a school's purchasing account with large office supply stores.
- Using account information obtained from the original call—and sometimes the school's website—the fraudster makes a second call and bills the school's line of credit for a large order of laptops, hard drives, printer ink, and other items that can total more than $200,000.
- A U.S. shipping address is provided belonging to a third-party—someone who has been fooled into thinking they are working from home, for example, but is another victim of the group's social engineering tactics. The purchase will later be re-shipped to Nigeria. In some cases, the order is directed to the actual school, whereupon the scammer—posing as a representative of the retail store—contacts the school and says the shipment was sent in error. The school, believing it is returning the order to the store, reships the items to a domestic address provided by the fraudster.
- Either way, once the fraud is discovered, it's too late, and the retailer absorbs the loss.

Those who perpetrate school impersonation schemes are members of an African Cyber Criminal Enterprise (ACCE), said Lipetsker, who has been investigating these groups for the past year as part of a new initiative in our Criminal Investigative Division.

ACCE refers to a network of predominantly Nigerian criminal actors who are engaged in computer-assisted frauds. The schemes are heavy on deception instead of hard-core intrusions, Lipetsker said. "The Africans don't do a lot of hacking," she explained. "They deceive their targets through phishing schemes and social engineering."

Lipetsker is part of our Asian, African, Middle-Eastern Criminal Enterprise Operations Unit, and she and other investigators and intelligence analysts work to stop cyber-assisted transnational crimes. "Our goal is to take down the entire criminal enterprise," she said, "not just a few actors."

Although many people equate Nigerian fraud schemes with ham-handed e-mail scams, ACCE members use sophisticated techniques to fool their targets, and they create forged online documents that are extremely convincing.

"They know where the vulnerabilities are," Lipetsker said, adding that many school systems make the fraudsters' job easier by posting information on their websites about their schools, personnel, and purchasing accounts.

"The greatest lesson that comes from this scheme is that retailers and schools systems must be vigilant about telephone and online orders," she said. "If you get large orders, make sure to independently verify the information. Don't just call the telephone number on the e-mail you received or be convinced by someone using the name of a known purchasing officer." She added, "A little diligence could save a lot of money and aggravation later."

FBI, DHS Offer Partners Terrorist Incident Response Training

Coordination Among Agencies is Key

Last September, al Shabaab gunmen attacked a shopping mall in Nairobi, Kenya, killing more than 70 people. In response, the FBI secured operational resources to assist Kenyan authorities.

Not long after, the Bureau—in partnership with the Department of Homeland Security (DHS)—formulated plans for a training exercise series to ensure that American law enforcement, other public safety first responders, and private sector entities had coordinated, effective response plans in place in case this type of complex terror attack ever occurs at a U.S. public venue.

These exercises aren't in response to any current threat but are simply part of our continuing mission to share information and work with public safety and private sector partners to improve overall threat response capabilities.

The first two phases of this training series took place last fall. Tabletop exercises were held with FBI field office personnel; federal, state, and local public safety officials; and private sector partners—including mall managers and owners—to discuss a hypothetical terror attack on a local mall and gain a clearer understanding of each other's capabilities and responsibilities. A second exercise was more inwardly focused, concentrating on FBI field office response plans and the effectiveness of our capabilities to communicate vital information to our own personnel and external partners.

After the training last fall, more effective responses to several subsequent public venue incidents—including an active shooter situation at a Maryland shopping mall this past January—were reported.

Lessons learned from Phases I and II were integrated into the third phase of the training, which is actually occurring now and over the next couple of weeks. During Phase III, FBI field offices—with DHS—are hosting a boots-on-the-ground exercise with regional federal, state, and local public and private sector partners at shopping malls outside of regular business hours.

This exercise scenario, like the first two phases, involves a simulated terrorist incident with numerous attacks, improvised explosive devices, and multiple victims and witnesses. Participants gather to discuss what's about to happen, run through the exercise, and finish up by reflecting on what worked and what didn't. After the several-hour exercise and the formal after-action review, participants will take the lessons learned and modify their own agency's response plans as needed to ensure they mesh with those of other agencies.

FBI Sacramento SWAT team members participate in a complex mall attack training exercise.

A few FBI offices have already conducted their Phase III training and can attest to its value.

For example, Monica Miller, special agent in charge of our Sacramento Division, said that her office's exercise "ensures unity and strategic collaboration among federal agencies, first responders, and private sector partners during a crisis" and also offered the opportunity to "make improvements well in advance of a real-world incident."

Also supportive was the general manager of the mall where the Sacramento exercise took place. "We take our participation in training exercises such as this one seriously," Eddie Ollmann explained, "because we know they help prepare our community to respond to potential emergency situations."

So far, all of this training has been regionally based. Later this year, the FBI will host a capstone exercise to incorporate national assets and resources into the mix in the event of a public venue attack with broader implications.

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

Left: A 586 Social Security card and credit card used in Sang-Hyun "Jimmy" Park's multi-million-dollar fraud scheme.

Sophisticated Fraud Scheme Dismantled

Ringleader Sentenced to 12 Years in Prison

The leader of a large-scale fraud ring who profited by helping people establish fake identities—enabling them to charge millions of dollars on credit cards they had no intention of paying off—was recently sentenced to 12 years in prison after pleading guilty to the charges against him.

The fraud carried out by New Jersey resident Sang-Hyun "Jimmy" Park was sophisticated and also brazen. He actively recruited scores of participants by placing ads that promised easy credit and easy money in Korean-language newspapers.

The scam hinged on Social Security cards that had 586 in the prefix. These were legitimate documents issued in the 1990s mostly to Chinese nationals hired to work in American territories such as Guam and American Samoa. When the workers returned to China, criminals there bought the so-called 586 cards, knowing they might illegally profit from them.

The criminals gathered more than 20,000 of the second-hand cards and then found buyers for them throughout the United States. In the New Jersey area, Jimmy Park was buying all the 586 cards he could get.

"He realized he had a clean slate with perfectly valid Social Security numbers," said Special Agent Barbara Woodruff, one of a team of investigators who worked the case out of our Newark Division. "Park understood the potential for financial gain and took it to the next level."

Here's how the scam worked:

- Park and his conspirators sold 586 cards for a fee, promising to help customers use the cards to get other forms of identification, including driver's licenses.
- With new identities in place, Park helped customers establish credit through a lengthy process. One of the methods was temporarily adding a new identity to an existing credit card account whose owner had excellent credit. The owners of the legitimate accounts were paid a fee for this service.
- After building the credit scores associated with the new identities—and detaching them from the legitimate accounts—Park helped customers obtain credit cards and open bank accounts.

"With valid credentials and high credit scores, the 586 card owners could open credit accounts everywhere—banks, retail stores, car dealerships," said Special Agent Theresa Fanelli, another member of the investigative team. "The sky was the limit."

The scammers then proceeded to "bust out" their credit cards, charging as much as $30,000 per month. "With an impeccable credit history," Woodruff explained, "none of the financial institutions batted an eye. Why would they?"

When it came time to pay monthly bills, the scammers made online or telephone payments using accounts that had no money behind them—knowing that the banks and retail outlets could take several days to figure out that the payments were bogus. During that period, they charged even more items.

"They were able to steal millions of dollars in a short amount of time," Fanelli said.

Park and his conspirators also paid merchants to charge sums on the fraudulent credit cards when no actual transactions took place. After receiving money from the fake sales in their accounts, the merchants gave the proceeds to Park, minus their cut.

Our investigation began at the end of 2008 after clues about the fraud were discovered during a homicide investigation. Arrests were made in September 2010. In all, 54 individuals were charged with various felony frauds, and most have pled guilty. Park admitted to defrauding numerous companies out of millions and was sentenced in February. After completing his prison term, he will be deported to South Korea.

Investigating Child Abductions

FBI CARD Team Plays a Vital Role

When a child goes missing, it impacts the whole community. And while local law enforcement and investigators from our regional FBI offices respond and begin looking into the disappearance, the Bureau has an additional investigative asset that can be called upon for these time-sensitive cases—our national Child Abduction Response Deployment (CARD) team, which works to recover victims as quickly as possible and helps apprehend those responsible for taking them.

The CARD team, created in 2006, has been deployed more than 100 times for approximately 108 victims, both domestically and—when requested—abroad. Numerous children have been located and safely returned to their loved ones. Tragically, the remains of victims have also been found—though this can at least provide some sort of closure for their families.

The 60 or so agents who make up the CARD team are stationed at field offices around the country. Each is assigned to one of five regional teams that cover the Northeast, Southeast, North Central, South Central, and Western United States and are deployed at the request of a field office. Deployment size depends on the case and the particular needs of local responders.

CARD team investigators are seasoned veterans of crimes against children cases—especially child abductions—and have received extensive training. While some local law enforcement agencies may only work one or two child abduction cases a year, CARD team agents work these kinds of cases all the time, keeping their unique skill set honed.

They often deploy to the abduction site with FBI behavioral analysis experts and technical specialists in tow. CARD team agents also work closely with National Center for the Analysis of Violent Crime coordinators, members of the regional FBI-led Child Exploitation Task Forces, and representatives from our Violent Crimes Against Children Section at FBI Headquarters.

What exactly does the CARD team bring to the table? In addition to being on the scene within an hour or two to augment local resources, these agents can quickly establish on-site command posts to centralize

investigative efforts. They also help map registered sex offenders in the area, handle national and international leads, guide investigative efforts using the protocols from the FBI's child abduction response plan, coordinate forensic resources as needed, and incorporate the Bureau's technical assets—which play an increasingly larger role in investigations where every minute counts.

But the true measure of the CARD team's impact is how often these kids are found safe. Here are a few recent examples where that's happened:

- A newborn kidnapped from his Wisconsin home in February 2014 was found by law enforcement the following day—alive—in a plastic storage crate outside a gas station in Iowa. The alleged kidnapper has been charged.
- In August 2013, a San Diego County teenager abducted by a family friend was located and rescued by law enforcement a week later in the Idaho wilderness. Her kidnapper, killed during the rescue, was believed to have been responsible for the deaths of her mother and 8-year-old brother.
- A 6-year-old girl, abducted from her Mississippi school in April 2013, was released the following day. The mastermind of the kidnapping received a 25-year prison term, while five other co-conspirators have also been sentenced.

While the FBI necessarily focuses on terrorism and other national security issues and major criminal threats, we will always place a premium on the safety and well being of our nation's children.

Remembering Our Fallen Agents

Training Accident at Sea Occurred One Year Ago

This month marks the one-year anniversary of the deaths of Chris Lorek and Stephen Shaw, special agents and members of our Hostage Rescue Team who were killed during a training accident off the coast of Virginia.

The two will be honored this week—during National Police Week—and their names will be installed in the FBI's Hall of Honor, a tribute to fallen agents killed in the line of duty throughout the Bureau's history.

As boys, both Chris and Steve dreamed of becoming FBI agents. They achieved that goal and then some, earning places on the Hostage Rescue Team (HRT), the Bureau's celebrated counterterrorism tactical unit that selects few members and undertakes dangerous missions around the globe.

"Chris and Stephen chose to be part of a team that assumes the greatest risk as part of their everyday job, a team that says, 'Yes, we will,' without any hesitation," noted former FBI Director Robert Mueller during a memorial service last year. "And though that kind of motivation—of service over self, even at the greatest cost—is difficult for some to comprehend, it is who they were, and it was in their very DNA, as it is with every member of HRT."

On May 17, 2013, during HRT training at sea near Virginia Beach, the two were fast-roping out of a helicopter when the aircraft encountered serious difficulties, causing the men to fall a significant distance into the water and suffer fatal injuries.

Left: Steve Shaw, left, and Chris Lorek were special agents and members of our Hostage Rescue Team.

News of the accident sent shockwaves through the HRT and the entire FBI. Chris, 41, and Steve, 40, were both married and each had two children. They lived near Quantico, Virginia, where the HRT is headquartered.

"It was an absolutely tragic day," said Jim Yacone, a former HRT operator and commander of the team. He now leads the Bureau's Critical Incident Response Group (CIRG), of which the HRT is a part. "Whether it's a training exercise or an actual mission, there are no acceptable losses."

Chris and Steve—like all their HRT colleagues—acknowledged and accepted the risks involved with being operators, Yacone explained. "They understood that HRT has to remain mission-ready at all times. They would not want us to stop training or preparing for the most extreme environments and circumstances."

Although the loss of the two popular and respected operators was a blow to the team, Yacone added that they will not be forgotten. "All of us will remember these two outstanding individuals and the contributions they made. Everybody has Chris and Steve in their memory, and that will be a driving force going forward. The team won't want to let them down."

The two are described by their HRT colleagues as talented, professional, and humble. "We have a dangerous job on HRT," one operator said. "In the back of your head you always know there's that ultimate risk, but it doesn't make their loss any easier." He added, "I know for all of us, it felt like we lost a family member, not just teammates."

Yacone suggested that while HRT operators will carry on with their mission, "they will know that Steve and Chris are watching—watching how we perform and how we stand up for them and their memory."

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

International Blackshades Malware Takedown

Coordinated Law Enforcement Actions Announced

Today, representatives from the FBI New York Field Office and the U.S. Attorney's Office for the Southern District of New York announced the results of a cyber takedown, which included the unsealing of an indictment against Swedish national Alex Yucel and the guilty plea of U.S. citizen Michael Hogue, both of whom we believe co-developed a particularly insidious computer malware known as Blackshades. This software was sold and distributed to thousands of people in more than 100 countries and has been used to infect more than half a million computers worldwide.

Also charged and arrested in the U.S. were an individual who helped market and sell the malware and two Blackshades users who bought the malware and then unleashed it upon unsuspecting computer users, surreptitiously installing it on their hardware. So far during the takedown, 40 FBI field offices have conducted approximately 100 interviews, executed more than 100 e-mail and physical search warrants, and seized more than 1,900 domains used by Blackshades users to control victims' computers.

And that's not all. The actions announced at today's press conference are part of an unprecedented law enforcement operation involving 18 other countries. More than 90 arrests have been made so far, and more than 300 searches have been conducted worldwide.

Malware is malicious software whose only purpose is to damage or perform other unwanted actions on computer systems. Blackshades malware—in particular, the Blackshades Remote Access Tool (RAT)—allows criminals to steal passwords and banking credentials; hack into social media accounts; access documents, photos, and other computer files; record all keystrokes; activate webcams; hold a computer for ransom; and use the computer in distributed denial of service (DDoS) attacks.

We uncovered the existence of the Blackshades malware during a previous international investigation called Operation Cardshop, which targeted "carding" crimes—offenses in which the Internet is used to traffic in and exploit the stolen credit cards, bank accounts,

U.S. Attorney for the Southern District of New York Preet Bharara announces arrests in the Blackshades malware cyber takedown during a press conference in New York.

and other personal identification information of hundreds of thousands of victims globally. We spun off a new investigation and ultimately identified one of the Cardshop subjects—Michael Hogue—and Alex Yucel as the Blackshades co-developers. Yucel, the alleged head of the organization that sold the malware, was previously arrested in Moldova and is awaiting U.S. extradition.

Our investigation revealed that several different types of Blackshades malware products were available for purchase by other cyber criminals through a website; the popular Blackshades RAT could be bought for as little as $40. In addition to its low price, the Blackshades RAT was very attractive because it could be customized by the criminals who bought it.

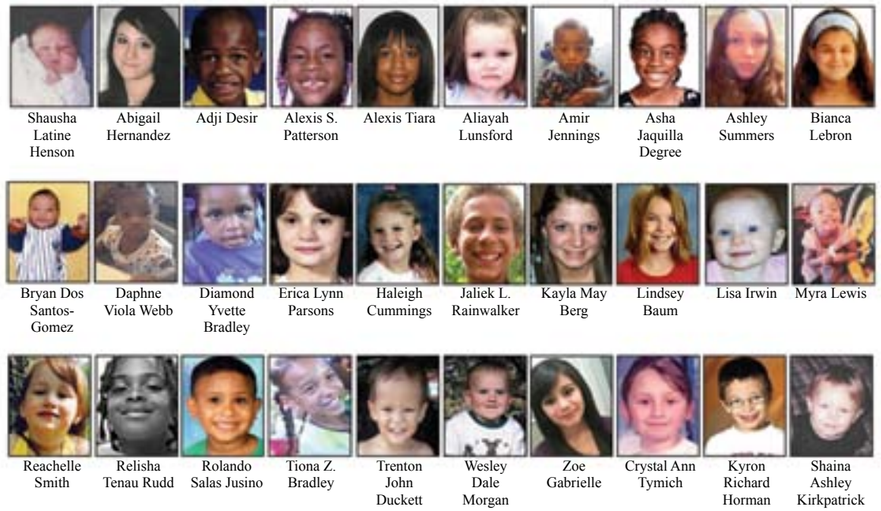
Yucel ran his organization like a business—hiring and firing employees, paying salaries, and updating the malicious software in response to customers' requests. He employed several administrators to facilitate the operation of the organization, including a director of marketing, a website developer, a customer service manager, and a team of customer service representatives.

New York FBI Assistant Director in Charge George Venizelos said that today's announcement "showcases the top to bottom approach the FBI takes to its cases… starting with those who put it [malware] in the hands of the users—the creators and those who helped make it readily available, the administrators."

We're currently working with Internet service providers to notify domestic victims of the Blackshades malware. But in the meantime, we're providing information on how to check your computer for a possible Blackshades infection at www.fbi.gov/blackshadesinfection.

Have You Seen These Kids?

National Missing Children's Day 2014



In observance of National Missing Children's Day on Sunday, May 25—which honors the memories of those who are lost and focuses attention on the issue—the FBI is highlighting the names and faces of the children listed on our Kidnappings and Missing Persons webpage and asking for your continued help to locate them.

We'd also like to remind everyone about the committed efforts the Bureau undertakes—in conjunction with our federal, state, local, and organizational partners—to help rescue the most vulnerable of crime victims, to bring to justice those who would harm them, and to educate parents and kids about the all-too-real dangers of violent and sexploitation crimes threatening children.

Those efforts include our:

- **National Child Abduction Rapid Deployment Team**, ready to travel anywhere at a moment's notice to assist in missing child investigations;
- **Innocence Lost National Initiative**, a partnership with the Department of Justice (DOJ) and the National Center for Missing & Exploited Children (NCMEC) that addresses domestic sex trafficking of children;
- **Child Exploitation Task Forces**, cooperative ventures with federal, state, and local partners around the country that investigate individuals and criminal enterprises responsible for victimizing young people;
- **Endangered Child Alert Program**, a joint effort with NCMEC that seeks national and international exposure of unknown adults whose faces and/or distinguishing characteristics are visible in child pornography images and videos;
- **Safe Online Surfing initiative**, a web-based program that teaches kids how to recognize and respond to online dangers like sexual predators and cyber bullying; and
- **FBI Child ID App**, which provides parents with an easy way to electronically store pictures and vital information about their children in case they go missing.

Recently, the NCMEC paid tribute to a number of Bureau employees—along with their state and local partners—for their extraordinary work on missing or exploited children investigations. We congratulate all the honorees, but we know our work is not done. The FBI will continue to make investigating violent crimes against young victims a priority, working side by side with our public and private partners to ensure the safety of children nationwide.

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

Investigating Student Aid Fraud

FBI Plays Supporting Role

It's a yearly spring ritual: college-bound students, young and old, applying online for much-needed federal student aid in the form of grants or loans.

Unfortunately, a few unscrupulous individuals view Title IV Federal Student Assistance funding as a way to line their own pockets—not to get an education. According to a recent assessment by the U.S. Department of Education's Office of Inspector General, the number of aid recipients potentially taking part in criminal fraud rings is increasing.

And while the FBI doesn't generally become involved these cases because of our necessary focus on counterterrorism, cyber crime, and other national security and major criminal threats, we do—as resources allow—assist our partners at the Department of Education and other agencies in rooting out some of the more egregious offenders. The Bureau brings to the table the same investigative methods and techniques we've used so successfully against criminals who commit other types of government fraud.

Why the increase in student aid fraud? For one, there are more online higher education opportunities—a single criminal participant can create multiple online student identities and apply for aid in each name. Another reason is the growing popularity of open access, lower-cost schools—like community colleges—where perpetrators can get back a larger percentage of a financial aid award in the form of excess Title IV funds (once the school applies the funds to tuition, anything left over is remitted directly to the "student" to use on related educational expenses like books, supplies, transportation, living costs, etc.).

It's not just the theft of millions of dollars of taxpayer money, though. Criminals committing federal student aid fraud are stealing enrollment slots from legitimate students and depriving qualified students of the Title IV funds they need. Those grants and loans sometimes make the difference between attending school and not attending school.

But the government and the higher education community are fighting back.

Recently, four people in Montgomery, Alabama were sentenced in federal court for their roles in a conspiracy to defraud the Department of Education and various colleges and universities of financial aid money. And just a week earlier, three defendants pled guilty to a federal student aid fraud scheme in San Francisco. The Bureau was involved in both cases.

Over the past several years, we've played a supporting role in a handful of other student aid fraud cases as well. For example:

- A Baltimore-area school test proctor and an admissions officer pled guilty in a scheme to manipulate test scores of students who were taking assessment exams to qualify for federal grants.
- A former inmate at a South Carolina prison pled guilty to applying for federal student aid using the identities of some of her fellow inmates.
- A San Diego college paid a civil settlement and its financial aid director pled guilty in connection with a scheme to submit falsified financial aid applications to obtain grants for students who were not eligible to receive them.

Investigative entities will continue to identify and bring to justice those who commit federal student aid fraud. And the Department of Education and colleges and universities will continue to put protections in place that make it harder to perpetrate these crimes.

Both actions will help ensure that federal student aid for higher education ends up in the hands of those who need and deserve it the most.

Bureau Initiative Focuses on Child Sex Tourism

Help the Victims, Apprehend the Abusers

Last month, the FBI asked for the public's help in a case involving a suspected serial child predator who for years taught in private international schools overseas. The suspect committed suicide after his employer saw pornographic images on his thumb drive, but as part of our subsequent investigation—when we began the process of identifying and notifying the victims shown in these images—we also asked that possible victims and others who may have information come forward, not only to aid investigators but to potentially access our victim assistance services.

Child sex tourism—people traveling to another country specifically to engage in illegal sexual conduct with children—is a very real issue that causes devastating and long-lasting psychological and physical consequences for victims. And the problem is growing, thanks to the relative ease of international travel coupled with the popularity of the Internet in helping individuals exchange information about how and where to find child victims in foreign locations.

The U.S. State Department estimates that more than a million children are exploited each year in the global commercial sex trade. That's in addition to the untold number of young victims of non-commercial sexual conduct.

But whether it involves commercial or non-commercial sex acts, the FBI—in conjunction with our domestic and international law enforcement partners—investigates U.S. citizens and permanent residents who travel overseas to engage in illegal sexual conduct with children under the age of 18. Since 2008, our Child Sex Tourism Initiative has employed proactive strategies to address the crime, including working with foreign law enforcement and non-governmental organizations to provide child victims with support services and to investigate and prosecute individuals engaging in child sex tourism.

The FBI also shares intelligence products with our overseas law enforcement partners that focus on trends, methods of operations, offenders, etc. And we offer training to foreign law enforcement and non-governmental organizations to build capacity and develop an effective team approach to address the problem. Intelligence sharing and training help develop cohesive multi-disciplinary teams, which in turn enable better international cooperation during the investigation of these crimes.

Children from developing countries are often seen as easy targets by Americans. Our investigations, however, have shown that American perpetrators travel to a variety of locations—from less developed areas in Southeast Asia and Central and South America to more developed areas in Europe. But it makes no difference where these crimes occur—any U.S. citizen or permanent resident who engages in sexual contact with a minor overseas is subject to prosecution under various U.S. laws.

And these laws were strengthened in 2003 with the passage of the federal PROTECT Act, which authorized a variety of additional prosecutive remedies and other tools to use against those who victimize children. It also makes clear that there is no statute of limitations for crimes involving the abduction or physical or sexual abuse of a child.

So a word of warning to perpetrators of this horrendous crime: No matter where you go, no matter how long it takes, you will be caught and prosecuted to the fullest extent of the law.

And a word of comfort to the victims: The FBI will work with your country's authorities and non-governmental organizations to bring perpetrators to justice and to help coordinate the services you need.

GameOver Zeus Botnet Disrupted

Collaborative Effort Among International Partners

On June 2, 2014, the Department of Justice and the FBI announced a multinational effort to disrupt the GameOver Zeus botnet, believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world.

Also announced was the unsealing of criminal charges in Pittsburgh and Omaha against alleged botnet administrator Evgeniy Mikhailovich Bogachev of Anapa, Russian Federation.

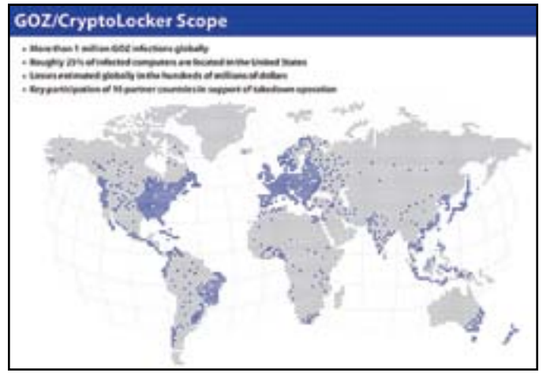
GameOver Zeus is an extremely sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects. It's predominately spread through spam e-mail or phishing messages.

Unbeknownst to their rightful owners, the infected computers become part of a global network of compromised computers known as a botnet—a powerful online tool that cyber criminals can use for their own nefarious purposes. In the case of GameOver Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. Losses attributable to GameOver Zeus are estimated to be more than $100 million.

Unlike earlier Zeus variants, GameOver has a decentralized, peer-to-peer command and control infrastructure rather than centralized points of origin, which means that instructions to the infected computers can come from any of the infected computers, making a takedown of the botnet more difficult. But not impossible.

Officials announced that in addition to the criminal charges in the case, the U.S. obtained civil and criminal court orders in federal court in Pittsburgh authorizing measures to sever communications between the infected computers, re-directing these computers away from criminal servers to substitute servers under the government's control.

The orders authorize the FBI to identity the IP addresses of the victim computers reaching out to the substitute servers and to provide that information to Computer



Emergency Readiness Teams (CERTs) around the world, as well as to Internet service providers and other private sector parties who are able to assist victims in removing GameOver Zeus from their computers.

Important note: No contents of victim communications are captured or accessible in the disruption process.

In a related action announced today, U.S. and foreign law enforcement officials seized Cryptolocker command and control servers. Cryptolocker is a type of ransomware that locks victims' computer files and demands a fee in return for unlocking them. Computers infected with Cryptolocker are often also infected with GameOver Zeus.

Evgeniy Bogachev, added to the FBI's Cyber's Most Wanted list, was identified in court documents as the leader of a gang of cyber criminals based in Russia and the Ukraine responsible for the development and operation of both the GameOver Zeus and Cryptolocker schemes.

The actions to take down GameOver Zeus were truly collaborative. "GameOver Zeus is the most sophisticated botnet the FBI and our allies have ever attempted to disrupt," said FBI Executive Assistant Director Robert Anderson. "The efforts announced today are a direct result of the effective relationships we have with our partners in the private sector, international law enforcement, and within the U.S. government."

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

Protecting Aircraft from Lasers

Trial Program Being Expanded Nationwide

After a successful trial program aimed at deterring people from pointing lasers at aircraft—by rewarding those who provide information about individuals who engage in this dangerous crime and aggressively prosecuting the perpetrators—the FBI is expanding the campaign nationwide.

"Aiming a laser pointer at an aircraft is a serious matter and a violation of federal law, said Joe Campbell, assistant director of our Criminal Investigative Division. "The public awareness campaign we launched in February has been effective in reducing the number of incidents, and our hope in expanding the program is that people will think twice about illegally using these devices."

A key part of the publicity campaign is reward money. For the next 90 days, the FBI will offer up to $10,000 for information leading to the arrest of any individual who intentionally aims a laser at an aircraft.

"We want to encourage people to come forward when they see someone committing this crime, which could have terrible consequences for pilots and their passengers," said George Johnson, a federal air marshal who serves as a liaison officer with the Bureau on laser issues.

The original initiative, which began nearly four months ago, took place in 12 FBI field offices where "lasing" incidents are prevalent. Since then, there has been a 19 percent decrease in the number of reported incidents in the major metropolitan areas of those offices.

Now, the Bureau—along with the Federal Aviation Administration (FAA) and the Air Line Pilots Association, International—are extending the program to all 50 states, Guam, and Puerto Rico. We are also working with state, local, and international law enforcement on the campaign, and we are conducting outreach to schools to educate teens about the dangers associated with lasing.

When aimed at an aircraft, the powerful beam of light from a handheld laser can travel more than a mile and illuminate a cockpit, disorienting and temporarily blinding pilots. Those who have experienced such attacks have described them as the equivalent of a camera flash going off in a pitch black car at night. As of December 2013, the FAA had documented at least 35 incidents where pilots required medical attention after a laser strike.

Interfering with the operation of an aircraft has long been a federal crime, but in 2012, a new law made it a felony to knowingly point the beam of a laser at an aircraft. The new law lowered the threshold for prosecution, Johnson said, "and the trend is on the rise for jail time in these cases."

In March, for example, a 26-year-old California man was sentenced to 14 years in prison for aiming a laser pointer at a police helicopter and a hospital emergency transport helicopter. The man and his girlfriend were using a device that was 13 times more powerful than the permissible power emission level for handheld lasers. The girlfriend was also convicted and recently sentenced to a two-year prison term.

Since the FBI and the FAA began tracking laser strikes in 2005, there has been more than a 1,000 percent increase in the number of incidents with these devices, which can be purchased in stores or online for as little as a few dollars. Last year, 3,960 laser strikes against aircraft were reported. It is estimated that thousands of attacks go unreported every year.

If you have information about a lasing incident or see someone pointing a laser at an aircraft, call your local FBI office or dial 911.

Operation Bodyguard

FBI Recognizes WWII Counterintelligence Landmark in New York

In honor of the 70th anniversary of the D-Day invasion, the FBI last weekend celebrated a landmark that was home to one of the Bureau's intelligence successes during World War II. At a ceremony in recognition of the effort of FBI employees during World War II, the Society of Former Special Agents, the Episcopal Diocese of New York, the Suffolk County Historical Society, and the FBI's New York Division placed a plaque at a quaint building known as Benson House in Wading River, New York, overlooking Long Island Sound.

It was there, from January 1942 until the end of the war in Europe in 1945, that FBI agents and radio technicians lived and worked undercover, secretly transmitting coded messages that the Nazis believed came from their own spies operating in New York. The Nazis believed their operatives were funneling significant details about U.S. forces, munitions, and war preparations. But in fact, the transmissions were controlled by the FBI—the Nazi spies were FBI double agents. The Bureau's work—known as Operation Ostrich—was central to our counterintelligence operations throughout the war and was part of a larger effort by Allied Forces to deceive the enemy called Operation Bodyguard.

The Allied effort derived its name from a statement by British Prime Minister Winston Churchill, who said, "In wartime, truth is so precious that she should always be attended by a bodyguard of lies."

Misleading Adolf Hitler's intelligence services was integrated into the long preparation for the June 6, 1944 landing of 160,000 Allied troops in Normandy, France. Operatives set out to deceive the Nazi leader about the nature and location of the main Allied thrust so that he would be ill-prepared to meet the invasion. The key to Bodyguard's success was the Allies' control of a number of German spies and ability to read coded German messages that confirmed the Nazis didn't know their agents were compromised.

For the FBI, the initial purpose in participating in the counterintelligence effort was to learn about Nazi espionage—who was involved, how they worked, and what they wanted to know. Early on, intelligence from

During World War II, FBI agents and radio technicians lived and worked undercover at Benson House, secretly transmitting coded messages that the Nazis believed came from their own spies.

one double agent's transmission indicated the Nazis were very interested in U.S. experiments with atomic energy. This, in part, spurred U.S. efforts to build the atomic bomb before the Nazis could.

The secretive work at Benson House proved even more valuable because it allowed us to plant misleading information for Nazi officials—essentially controlling what the enemy knew about the U.S. and its state of military readiness. In the case of Operation Bodyguard, it allowed us to help Allied efforts to protect the D-Day invasion plans.

Even after the fall of Germany in 1945, Nazi intelligence officials believed that the hundreds of messages sent by their spies in the U.S. were real. The FBI's efforts to contribute to the Allied "bodyguard of lies" were among the many Bureau intelligence efforts during the war and were surely some of our most significant.

A plaque placed at Benson House in honor of the 70th anniversary of the D-Day invasion recognizes the counterintelligence efforts of FBI employees during WWII.

The Testing That Wasn't

New York Man Falsifies Test Data on Military Equipment

Technology enhances the U.S. military's ability to protect our nation. That technology, however, is traditionally subject to stringent testing measures to ensure it operates the way it's supposed to.

Unfortunately, one testing manager employed by a government contractor in western New York decided, on his own, that the testing requirements imposed by the Department of Defense (DOD) on his company were unnecessary, so he cut corners. And when the FBI and our military partners got wind of his actions, the ensuing joint investigation resulted in that testing manager's guilty plea and subsequent federal prison term. He was also ordered to pay nearly $300,000 in restitution for the retesting costs incurred by the military.

Steve Wysocki personally oversaw product testing for two specific projects—the KG-40 military radio system and the SH-60 Sonobuoy system. The KG-40 is a tactical radio encryption system used by the U.S. Army and Navy and also sold for export to foreign countries, while the SH-60 is an anti-submarine warfare device that includes a small sonar unit usually released into the ocean from an aircraft.

In 2011, the FBI received information about possible falsification of testing data for the KG-40 radio system. Teaming up with investigators from the Army Criminal Investigation Division's Major Procurement Fraud Unit, the Naval Criminal Investigative Service, and the Defense Criminal Investigative Service, we began looking into the allegations.

The investigation, which involved extensive reviews of company testing records and numerous interviews with company employees and others, revealed how the data was falsified. Here's how it worked:

- Among the testing protocols imposed by DOD for the KG-40 and SH-60 is something called vibration testing—component parts being placed on a vibration table for a certain period of time to ensure they can survive real-world combat conditions on aircraft and ships.
- During vibration testing, the components are hooked up to a computer that monitors performance and produces a profile. Because of testing variables, no two items will produce the same exact testing profile.
- Wysocki admitted to personally falsifying vibration test profiles—and directing subordinates to do the same—for components of the KG-40 and SH-60 systems by using testing profiles from previous items and simply changing the serial number, date, and time of the test. These phony profiles were then inserted into each component's "traveler file," which accompanies it throughout the assembly and testing process. Each tested item needs a copy of a passing vibration table profile in its file before it can be released to the military. Wysocki even had a name for his non-testing procedure: "phantom vibe testing."
- To justify the phantom vibe testing to his workers, Wysocki told them that the testing of certain components could be skipped because those types of components had no reported failures detected during vibration testing. He also told them he was trying to clear up a backlog and that the units needed to move along the line quicker.

But no matter how Wysocki tried to justify his actions to his subordinates—or perhaps to himself—he broke the law. And as U.S. Attorney William Hochul, Jr., Western District of New York, put it, "This office will not tolerate anybody who, by their actions, hurts or impacts the products used by our military men and women to carry out their critical mission."

Public Corruption Update

FBI Continues Efforts to Root Out Crooked Officials

The vast majority of public servants who work at the local, state, and federal levels of government are honest and dedicated folks who strive every day to do the right thing for their constituents, their communities, and their country.

Unfortunately, there is a small subgroup of public servants who, whether elected, appointed, or contracted, are only concerned about a very specific constituency—themselves. And because this type of corruption strikes at the heart of government, eroding public confidence and undermining the strength of our democracy, the investigation of public corruption is the FBI's top criminal priority.

Currently the Bureau is working more than 4,000 public corruption cases around the nation with the help of our partners. Our investigative efforts pay off year after year—fiscal year 2013 alone saw approximately 1,200 federal indictments and informations against corrupt officials.

Investigating the corruption of federal personnel—in particular, trusted officials and employees with access to sensitive information—is our number one public corruption priority because of the potential impact on U.S. national security. But corrupt state and local officials—who, like their federal counterparts, take an oath to serve—can seriously harm public trust in government. They can also jeopardize public safety and waste millions of taxpayer dollars.

The FBI is uniquely situated to investigate public corruption—we've got plenty of experience and the resources to run the kind of long-term, complex investigations that corruption activities often require. To uncover secretive activities like bribery, embezzlement, racketeering, kickbacks, and money laundering, we use sophisticated investigative techniques that can give us a front row seat to handshakes, money exchanges, or descriptions of corrupt schemes directly from the mouths of the officials involved. These techniques—which we've been using successfully for years against organized crime—include electronic surveillance, undercover operations, and informants/cooperating witnesses.

However, investigating public corruption is an FBI commitment as old as the Bureau itself. When we were founded in 1908, our responsibilities included the investigation of land fraud, which often involved corrupt public officials.

Because of the nature of public corruption, we work closely with the Department of Justice's Public Integrity Section and U.S. Attorney's offices to ensure laws, guidelines, and protocols are strictly adhered to during investigations.

Where do our cases come from? Sometimes from credible information from a Bureau source. Or we might uncover something about unrelated corruption activities during a public corruption investigation and spin that off into a new case. We receive complaints from citizens. Disgruntled participants in corruption schemes sometimes come to us and tell us what they know. And occasionally, the corrupt official might self-report, hoping for leniency from the government.

And if a determination is made that the reported activity doesn't rise to the level of federal prosecution, we can and do refer cases to state attorneys general offices or local prosecutors.

Public corruption, though, is not just an American problem—it plagues countries around the world. So the FBI offers training to foreign law enforcement, prosecutors, and judges through our International Law Enforcement Academy in Budapest, several other international academies, and our National Academy program at Quantico, Virginia.

In the U.S. and abroad, the FBI is doing everything we can to help ensure that the good name of the vast majority of public servants is not besmirched by a corrupt few.

A Byte Out of History

50 Years Since Mississippi Burning

Fifty years ago, our country was in the midst of a struggle to extend full rights and liberties to all of its citizens. On the national stage, the long legislative fight on the landmark Civil Rights Act was nearing a conclusion. Regionally, the push to roll back odious Jim Crow laws led to demonstrations between opponents of the legal discrimination and supporters of the status quo.

In Mississippi, the center of the civil rights effort in 1964 was the Freedom Summer, in which committed activists and local residents encouraged African-Americans to register to vote—fewer than seven percent of those eligible were registered at the time. The Council of Federated Organizations (COFO), a coalition of civil rights groups, arranged the drive, and orientation for its registrars had begun in mid-June.

Michael Schwerner, a 24-year-old social worker, had just started a job with the Congress on Racial Equality in Mississippi and quickly came to the attention of local Klan members. He had been at the Freedom Summer training in Ohio and was returning to Mississippi with fellow activists Andrew Goodman and James Chaney. Their plan was to visit Mount Zion Church in Neshoba County, which had been burned by the Klan.

Arriving in Philadelphia, Mississippi on June 21, the three were arrested by Deputy Sheriff Cecil Price, who charged Chaney with speeding and held the other two "for investigation." Though the men were released from custody later that night and set off for their lodgings, they were followed out of town. They never made it to their destination.

Left: The burned interior of the station wagon that was discovered following the disappearance of activists Michael Schwerner, James Chaney, and Andrew Goodman.

Even before that, their friends at COFO had become concerned. Schwerner's travel plans indicated the three would arrive at their hotel that afternoon. When they missed 4 p.m. check-in, COFO began to try and track their whereabouts, calling around the county throughout the evening. By 10 p.m., around the time they were released, COFO still hadn't heard from them and relayed their concerns to the local FBI and a Department of Justice representative who was in the area. At that point, though, nothing was known of the three or about what had happened. Without evidence to suspect foul play, there were no grounds yet for FBI involvement.

But in this case, the ramifications were not just a local matter. The voting rights drive in Mississippi and its national implications were clearly on the radars of President Johnson and Attorney General Robert Kennedy, who took great interest in civil rights matters. Although the FBI's local agent had begun asking about the missing workers on June 22, the Justice Department wanted even more involvement and told the FBI to place additional agents on the case.

By the next day, another 10 agents had been assigned to the case. The FBI received a tip about a burning station wagon seen in the woods off of Highway 21, about 13 miles northeast of Philadelphia—it was the men's vehicle. Soon after the find, FBI Director J. Edgar Hoover was advising President Johnson on the case. With no remains found in the car, there was a slim hope that the three might still be found alive. President Johnson informed the Schwerner family and closely followed the FBI's progress.

The Mississippi Burning, or MIBURN, case quickly became one of the Bureau's biggest investigations; FBI resources and personnel that moved into Mississippi that summer—including the opening of the new FBI field office in the state capitol—reflected the massive effort.

Operation Cross Country

Recovering Victims of Child Sex Trafficking

In many ways, Nicole was a typical teenager. In high school she tried cigarettes and alcohol, but she says, "I was pretty much a good kid. I didn't really stay out late, I always came home, I never stole anything. I did what a lot of teenagers do."

By age 17, however, things were deteriorating at home. Her parents were divorced, her father was absent, and she and her mother had an on-again, off-again relationship. That's when Nicole met a man who took her shopping and showered her with attention. "He was gorgeous and he had charm," she said. "I didn't really think he was going to turn out to be…" Her voice trailed off as she tried to find words to describe Juan Vianez, the pimp who forced her into prostitution and later brutally beat her.

Now 27, Nicole is one of countless young women victimized by child sex traffickers. But with the assistance of the FBI and our partners, she and other victims are turning their lives around—and helping to put hundreds of pimps behind bars.

Operation Cross Country, an annual law enforcement action that took place last week in 106 U.S. cities, highlights ongoing efforts by the Bureau—together with the National Center for Missing & Exploited Children and our local, state, and federal law enforcement partners—to address the sexual exploitation of juveniles as part of our Innocence Lost National Initiative.

Since its creation in 2003, the Innocence Lost program has resulted in the identification and recovery of approximately 3,600 minors who have been sexually exploited. **This year marks the eighth Operation Cross Country, the largest such enforcement action to date: 168 trafficking victims were recovered and 281 pimps were arrested.**

"These are not children living in some faraway place, far from everyday life," FBI Director James Comey said at a press conference today at FBI Headquarters. "These are America's children."

To address violent crimes against children, the FBI has established nearly 70 Child Exploitation Task Forces around the country, said Special Agent Steve Vienneau. Noting that the task forces rely on partnerships with all levels of law enforcement, Vienneau added, "the FBI could never succeed in this mission alone." The task forces also include FBI victim specialists from our Office for Victim Assistance—men and women who play a key role in helping victims while their cases are being investigated and up to and beyond criminal prosecutions.

Nicole was 17 when she was lured into a life of forced prostitution by a man who initially charmed her but turned out to be a pimp.

"We don't enter any of our victims' lives at a good time," said Victim Specialist Dani Geissinger-Rodarte, who works in our Seattle Division and who was instrumental in helping Nicole get away from her pimp and later testify against him (Vianez is serving a 20-year jail term).

"A lot of victims of child prostitution have difficult backgrounds," Geissinger-Rodarte explained, so victim specialists must assess the girls' needs before they can begin to help them.

Sometimes, it's not easy to convince young victims they need to get away from those who are exploiting them. Nicole, like many trafficked juveniles, was totally dependent on her pimp. "I didn't have money, I didn't have a house, I didn't have a bank account, I didn't have my own car," she said. "I didn't have anything. So if I left Juan, I left everything."

In 2007, after a vicious beating that left her in the hospital with serious injuries, Nicole met Geissinger-Rodarte—and over time came to trust her. Eventually, Geissinger-Rodarte connected Nicole with community services and helped her to see there was a future beyond prostitution.

Today, Nicole is an honors college student on her way to a psychology degree. She has a job, a driver's license, a good credit rating, and she just bought a new car. "I am very, very proud of myself," she said.

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

Bank Guilty of Violating U.S. Economic Sanctions

Record Penalties Levied Against Global Financial Institution

France's largest bank—and the fourth largest financial institution in the world—has admitted to large-scale, systematic exploitation of the American financial system on behalf of countries facing U.S. economic sanctions (such as Sudan, Iran, and Cuba) and has agreed to pay record penalties of nearly $9 billion.

BNP Paribas (BNPP), a global financial institution headquartered in Paris, has admitted its role in violating the International Emergency Economic Powers Act and the Trading with the Enemy Act by processing billions of dollars of transactions through the U.S. financial system on behalf of entities subject to U.S. economic sanctions.

"BNP Paribas went to elaborate lengths to conceal prohibited transactions, cover its tracks, and deceive U.S. authorities," noted Attorney General Eric Holder during a press conference yesterday at the Department of Justice in Washington, D.C. "These actions represent a serious breach of U.S. law."

According to documents released yesterday, from 2004 until 2012, BNPP illegally moved more than $8.8 billion through the U.S. financial system on behalf of sanctioned entities and used a variety of schemes to conceal the true nature of the transactions from U.S. regulators.

For example, BNPP routed illegal payments through third-party financial institutions to conceal the involvement of the sanctioned entities as well as BNPP's role in the transactions. In addition, the bank instructed other financial institutions not to mention the names of sanctioned entities in payments sent through the U.S. and removed references to those entities from payment messages, thereby enabling the funds to pass through the U.S. financial system undetected.

Left: As Attorney General Eric Holder (right) looks on, FBI Director James Comey speaks at a press conference announcing charges against BNP Paribas, which has agreed to plead guilty and pay $8.9 billion for illegally processing financial transactions on behalf countries subject to U.S. economic sanctions.

"The significant financial penalties imposed on BNP Paribas send a powerful deterrent message to any company that places its profits ahead of its adherence to the law," said FBI Director James Comey. "We will continue to work closely with our federal and state partners to ensure compliance with U.S. banking laws to promote integrity across financial institutions and to safeguard our national security."

During the course of the more than four-year investigation, FBI agents from our New York Division and criminal investigators from the Internal Revenue Service reviewed scores of financial documents and e-mails to unravel the illicit activity and made numerous trips overseas to interview people with knowledge of the transactions.

The majority of illegal payments were made on behalf of sanctioned entities in Sudan, which was subject to U.S. embargo based on the Sudanese government's role in facilitating terrorism and committing human rights abuses. BNPP processed approximately $6.4 billion through the U.S. on behalf of Sudanese sanctioned entities between 2006 and 2007, including approximately $4 billion on behalf of a financial institution owned by the government of Sudan, even as internal e-mails showed BNPP employees expressing concern about the bank's role assisting the Sudanese government.

In March 2007, a senior compliance officer at BNPP wrote to other high-level BNPP employees reminding them that certain Sudanese banks BNPP was dealing with "play a pivotal part in the support of the Sudanese government which…has hosted Osama Bin Laden and refuses the United Nations intervention in Darfur."

The case against BNPP "should send a strong message to any institution anywhere in the world that does business in the United States," Attorney General Holder said. "Illegal conduct will simply not be tolerated."

Violent Criminals Sentenced

Charged in 2010 Murder of Oklahoma Couple

In August 2010, Oklahoma retirees and high school sweethearts Gary and Linda Haas took off in their truck and travel trailer for their annual camping trip to Colorado. But tragically, they soon crossed paths with violent prison escapees and were murdered inside that trailer.

As a result of the FBI and New Mexico State Police-led investigation into this especially brutal crime, last month defendant John Charles McCluskey received a life sentence plus 235 years. His accomplices—fellow prison escapee Tracy Allen Province and Casslyn Mae Welch—McCluskey's girlfriend—were sentenced to five consecutive life terms and 40 years, respectively.

It began on July 30, 2010, when McCluskey, fellow inmate Tracy Allen Province, and a third inmate—all violent offenders—escaped from an Arizona state prison with the assistance of Welch. (The third inmate was separated from the others during the escape but was apprehended two days later.)

McCluskey, Province, and Welch—using handguns provided by Welch—kidnapped two truck drivers who had stopped along a nearby interstate and took their truck to Flagstaff. Leaving the truck drivers at a rest stop, the group then stole a small sedan to continue their getaway. But after driving in the small car with little or no sleep, the three thought it would be a good idea to target a camper or trailer owner, so on August 2, 2010, they pulled off at a New Mexico rest stop to find one.

Unfortunately, Gary and Linda Haas also chose the same rest stop. And it wasn't long before they were spotted by McCluskey and his accomplices, who carjacked the couple at gunpoint and forced them back onto the interstate.

A short distance later, McCluskey ordered the couple to exit the interstate and stop at a secluded location, where he shot and killed Gary and Linda Haas at point-blank range inside their trailer. The trio towed the trailer to another secluded location and set it on fire, with the Haases' bodies inside. They then took off in the couple's truck and drove to Albuquerque, where they abandoned it in a shopping center—but not before trying to wipe it down inside and outside to remove fingerprints.

This is all that was left of the travel trailer belonging to Oklahoma retirees Gary and Linda Haas when it was discovered in New Mexico in 2010. The couple was murdered inside the trailer by a escaped prison inmate and his accomplices.

On August 4, 2010, the New Mexico State Police discovered the remains of Gary and Linda Haas in their burned trailer. Later that day, they also located the couple's pick-up truck in Albuquerque. After a multi-state, multi-agency manhunt, Tracy Allen Province was apprehended in Wyoming on August 9, 2010, and McCluskey and Welch—thanks to an alert U.S. Forest Service employee—were apprehended at a camp ground in Arizona on August 19, 2010.

Collaborative evidence collection played a key role in this case. Personnel from the New Mexico State Police and the New Mexico Department of Public Safety Forensic Laboratory performed the initial crime scene work at the burned-out trailer and the victims' truck. Despite the criminals' attempts to wipe the truck clean, the three subjects were able to be identified through fingerprint and DNA evidence they left behind.

Then the FBI's Evidence Response Teams from our Phoenix and Albuquerque offices processed the location where McCluskey and Welch were apprehended as well as the stolen sedan they were driving. ERT personnel recovered several telling items owned by the victims, including the very handgun used to kill the couple and a cap belonging to Gary Haas that McCluskey was wearing at the time of his arrest.

Left: FBI Director James Comey speaks at the International Law Enforcement Critical Infrastructure Symposium in Miami on July 7, 2014. (Interpol Photo)

FBI, Interpol Host Critical Infrastructure Symposium

Director Comey Addresses the Importance of Partnerships

FBI Director James Comey was in Miami yesterday, where he spoke at the opening of the four-day International Law Enforcement Critical Infrastructure Symposium. The event, co-hosted by the FBI's Weapons of Mass Destruction (WMD) Directorate and Interpol, has drawn senior law enforcement officials from more than 90 countries to explore and share best practices for managing WMD and counterterrorism threats targeted against critical infrastructure and to identify common approaches to protect infrastructure and key resources.

Also participating in the symposium are domestic first responders, corporate security officers, and other U.S. federal partners.

"Today, critical infrastructure is all encompassing," said Director Comey. "It is everything to our country and our world—our dams, our bridges, our highways, our networks," he added, explaining that the threats we face to our interconnected systems—such as bioterrorism, agroterrorism, and sabotage—are as diverse as our infrastructure itself.

Comey cited examples of threats to infrastructure, to include the armed assault last April on a California power station, the 2008 attack in Mumbai in which gunmen opened fire at a number of locations, and last year's deadly shootings at a Kenyan shopping mall. He also noted the ninth anniversary of the July 7, 2013 strikes by terrorists who bombed the London Underground and a double-decker bus in a series of coordinated suicide attacks.

"We know these threats are real," Comey told the audience. "We must together figure out ways to protect our infrastructure, to work together to strengthen our response to a terrorist attack, a tragic accident, or a natural disaster."

While touching on topics ranging from terrorism, cyber, and WMD threats to training, partnerships, and intelligence, Comey's theme throughout underscored the importance of open communication and information sharing with our partners in the U.S. and abroad.

Interpol, as an international police organization, is an important partner on which the Bureau relies heavily to help combat threats of all types. The FBI, through its liaison with Interpol, is able to leverage 190 member countries to address challenges around the globe—a very important ability in a constantly evolving global threat environment.

Comey also highlighted the work of our WMD Directorate, each FBI field office's WMD coordinator, and our two regional WMD assistant legal attachés in Tbilisi and Singapore. "They integrate our counterterrorism, intelligence, counterintelligence, scientific, and technological components and provide timely analysis of the threat and response," Comey said. "The goal is to shrink the world to respond to the threat."

The symposium provides the opportunity for participants to help work toward that goal. Through networking and discussions on how to coordinate and cooperate on critical infrastructure preparedness and protection efforts, attendees will strengthen existing partnerships and develop new ones. By rallying the international community around defeating a common threat, our collective chances of success increase.

Director Comey said that our greatest weapon in this fight is unity, which is developed through intelligence sharing and interagency cooperation. "It is built on the idea that standing together, we are smarter and stronger than when we are standing alone," he said. "Because no one person—no FBI agent, no police officer, no agency, and no country—can prevent or respond to an attack on critical infrastructure alone."

Dog Fighting Ringleader Pleads Guilty

Multi-State Criminal Enterprise Shut Down

In 2011, our Mobile Field Office had received some disturbing reports about a possible high-stakes dog fighting and gambling enterprise based in Alabama with activities spanning several nearby states. So in April of that year, the Bureau—in conjunction with our law enforcement partners in those states—opened an investigation.

By August 2013, this broad and coordinated investigative effort—which involved sophisticated techniques like court-authorized wiretaps and confidential sources—had led to the indictment and arrest of 10 individuals on federal dog fighting and gambling charges. Several others were subsequently charged.

A key figure in this group of co-conspirators—Donnie Anderson—recently pled guilty in the case. In addition, nine others involved have pled guilty thus far.

In his plea agreement, Anderson admitted to organizing and holding dog fights—mostly in the Auburn, Alabama area—from 2009 to 2013, as well as charging spectators an entrance fee of between $100 to $150 (although owners of dogs fighting at that particular event got in for free). He also said that dog owners and spectators were betting on the outcome of the fights, putting up a total of anywhere between $20,000 and $200,000 per fight. And, Anderson admitted to not only hosting the fights but—along with his co-conspirators—buying, selling, transporting, housing, and training the dogs used in the fights.

Dogs involved in these matches are treated very poorly—they are neglected and abused, living primarily in cages or in chains without adequate food and water. During training, they're taught to attack live bait (often times stolen pets like cats, rabbits, and small dogs). After a fight, the losing dog is often killed.

And dog fighting (as well as cock fighting) is usually always accompanied by other illegal activities, like gambling, illegal firearms activity, and drug trafficking. During the August 2013 takedown of Donnie Anderson's operation, law enforcement personnel seized guns, illegal drugs, drugs used to treat and train dogs, and more than $500,000 in cash.

Along with the round-up of Anderson and his co-conspirators on that day, 367 dogs were rescued with the assistance of the American Society for the Prevention of Cruelty to Animals and the Humane Society of the United States. Most of the recovered dogs were in pretty bad shape, with plenty of evidence showing they had been subjected to fighting activities. But after medical treatment and rehabilitation, many of the dogs have been or are in the process of being placed into loving homes.

Federal enforcement of dog fighting activities in general got a boost in 2007 when the Animal Fighting Prohibition Enforcement Act—which targeted individuals directly involved in fighting activities—was passed. This law prohibits the interstate trafficking of animals that will be used for fighting and also strengthens imprisonment penalties.

But a word of warning to spectators at these events—this past February, a new federal provision made it a crime to knowingly attend an animal fighting event and to knowingly bring a child under the age of 16 to such an event.

In recognition of their actions that led to the rescue of hundreds of mistreated dogs, two FBI agents and a former agent—along with an Auburn Police Department detective and the U.S. Attorney and Assistant U.S. Attorney for the Middle District of Alabama—were all recently recognized with an award from the Humane Society.

A Byte Out of History

50th Anniversary of the FBI's Jackson Field Office

Fifty years ago this summer, Mississippi was at the front and center of our country's civil rights struggles, with cases such as the June 21, 1964 disappearance of three civil rights workers becoming issues of national concern. Less than two weeks later—and in response to that tragic event—the FBI opened its Jackson Field Office.

On July 10, 2014, FBI employees joined state officials, law enforcement partners, and civil rights era figures, including Myrlie Evers-Williams—widow of civil rights leader Medgar Evers, who was slain in Mississippi in 1963—in celebrating the 50th anniversary of our Jackson Division and the vital role the office has played since then in the Bureau's civil rights program.

Evers-Williams noted the long evolution of the fights and passions that led to the opening of the Jackson Field Office and the scars that those directly involved bore. "We saw the FBI only as an institution set to keep people of color down," she said. "One that was not a friend, but one that was a foe. And I stand before you today saying that I am proud to say I see the FBI as playing the role they did, and finally in my mind, and my heart reaching the point where I can say, friend."

This turning of foe to friend was set in motion 50 years ago under unique circumstances. Usually when an FBI field office is opened, the Bureau spends a significant amount of time analyzing the caseloads of nearby offices, comparing the geographic distribution of those cases, and evaluating where the most efficient place would be to put a new office.

Left: Director Hoover greets Jackson Police Department Chief W.D. Rayfield (left) and Jackson Mayor Allen C. Thompson (right) in the newly opened Jackson FBI Field Office on July 10, 1964.

The violence in Mississippi, though, demanded an immediate and strong response. In late June, an aide to President Lyndon Johnson called the FBI's White House liaison, Assistant Director "Deke" DeLoach, and told him that the president wanted the FBI's presence in Mississippi greatly increased. The president himself was telling FBI Director J. Edgar Hoover the same thing as Hoover reported in regularly on the case of the missing civil rights workers. On June 29, 1964, Hoover reported to Johnson, "I am opening a main office at Jackson, Mississippi…[but] it won't be able to be effective for three or four days."

FBI Memphis Special Agent in Charge Karl Dissly—at that time responsible for investigations in the northern part of Mississippi—was sent to Jackson to hunt for office space, but he faced some challenges. The Bureau needed suitable space, and quickly. And local prejudices meant that it might be hard to find a landlord willing to rent to an integrated agency—the FBI employed not only African-American support staff but also agents.

But these problems were worked out, and on July 10, 1964, Hoover arrived in Mississippi for the office's dedication. When speaking of the reasons for the office, Hoover said he knew that there were "strong feeling we were coming in to take over" and he wanted to allay those fears, explaining that the FBI would keep within bounds of the law and its mandate.

The creation of the Jackson Field Office, recognized last week, was a product of need, tragedy, politics, and especially passion—passion to oppose the violence and cruelty encouraged by the Jim Crow laws.

"Liberty and justice for all," said FBI Deputy Director Mark Giuliano, who also spoke at last week's ceremony, "that is what Jackson office stands for. It is what the FBI stands for."

Scan this QR code with your smartphone to access related information, or visit www.fbi.gov/jackson50th.

The Transnational Gang Threat

Part 1: Joining Forces to Meet the Challenge

The community activists, social workers, and police officers from six Central American countries and the U.S. who had arrived in the nation's capital the previous day were now assembled at the Eisenhower Executive Office Building next door to the White House. Chatting in Spanish and English, they waited for the official start of a two-week training program with an innovative approach to dealing with the problem of transnational gangs.

The FBI-led initiative known as CACIE—the Central American Community Impact Exchange program—unites civic groups and law enforcement organizations to deter gang violence and criminal activity by helping to keep young people from joining gangs. This deterrence model stresses prevention in addition to police intervention, and the 22 CACIE participants are on the front lines of that effort.

The MS-13 and 18th Street gangs are entrenched in many parts of Central America and are notoriously violent. Gang members in their teens are responsible for kidnappings and extortion, trafficking of drugs and people, and brutal murders. Often, a young person must kill someone before being fully admitted into the gang. And these crimes don't heed borders.

"The White House recognizes that violent crime and the illicit flow of drugs and money across borders can be a threat to America's national security," said George Selim, a member of the White House National Security Staff, which sponsors the CACIE initiative along with the FBI and the U.S. Department of State. "Community solutions, rather than government solutions," Selim said during CACIE's opening ceremony in April, "are really the spirit behind this effort."

The training program—the second since CACIE was established in 2013—brings together a cross-section of dedicated individuals involved in the fight against gangs. The goal is to share best practices about how to deter recruitment of gang members, whether through community-based after-school programs, police-sponsored youth corps, or other initiatives rooted in their respective communities. CACIE also promotes long-term partnerships between civic organizations and law enforcement agencies.

CACIE participants from Guatemala listen to a translation of events at the start of the two-week training program.

"We need to understand the enemy we are fighting," said Jason Kaplan, the FBI's legal attaché in El Salvador. "Gang members do not pay attention to borders. So we need to develop lasting and meaningful relationships with our international partners to deal with the gang threat." He added, "We have to establish programs to teach young people about the dangers of drugs and gangs and violent crimes. CACIE is all about prevention, and that is critical, because you can't arrest your way out of the gang problem."

Following the opening events in Washington, D.C., CACIE participants spent time at the FBI's training facility in Quantico, Virginia; in Durham, North Carolina, to learn about prevention programs that are working; and in Guatemala, where a new emphasis is being placed on community policing to fight the gang threat.

On the first day of their training, Legal Attaché Kaplan encouraged CACIE participants from Honduras, Guatemala, El Salvador, Belize, Costa Rica, Panama, and the U.S. "to walk away from this experience with plenty of business cards and good ideas. Everyone involved in the fight against transnational gangs has to be assertive," he said. "You will need to be champions for your countries and your communities, and for the young people who are growing up there right now."

Part 2: Building Partnerships That Last (page 56)

The Transnational Gang Threat

Part 2: Building Partnerships That Last

Wearing special headsets and sensors that transported them into a virtual world, the Central American Community Impact Exchange (CACIE) participants prepared to do battle in the FBI's simulation trainer. The armed criminals projected through their 3D goggles lurked behind furniture and doorways. Carrying real M4 rifles customized to shoot virtual rounds, it was the team's job to subdue the bad guys without becoming casualties themselves.

The state-of-the-art simulation trainer at our facility in Quantico, Virginia helps new FBI agents-in-training and police officers around the country hone their tactical skills. For the CACIE group—many of whom are not members of law enforcement—the simulator was an illuminating and sobering lesson in how dangerous a police officer's job is and how crucial teamwork is to success.

"Until today," said a community activist from Honduras who had just emerged from a training run in the simulator, "I had never held or fired a weapon in my life." Unfortunately, transnational gangs such as MS-13 and 18th Street use guns far too often for crimes and murders in her country and elsewhere in Central America.

One of CACIE's primary goals is to bring law enforcement and community groups together to develop programs that keep youths from being recruited by gangs. "The idea is to provide young people with other opportunities," said Special Agent Rich Baer, a member

Left: CACIE participants use the FBI's state-of-the-art simulation trainer in Quantico, Virginia to hone their tactical skills.

of the FBI's Safe Streets and Gang Unit who helps administer the CACIE program.

For that concept to work, the 22 CACIE participants from Honduras, Guatemala, El Salvador, Belize, Costa Rica, Panama, and the U.S. must develop strong relationships so that when the two-week class is completed, lasting partnerships can be formed.

"All the people here need to become close friends during this experience," said Gerry Lopez, a senior deputy district attorney in Riverside, California, who participated in the first CACIE training session last year and was invited back to share best practices with this year's class. "Before there can be an effective professional connection," he said, "there needs to be a meaningful personal connection."

That's why the team-building exercise in the virtual trainer—along with other classroom, tactical, and field training the group received—is vital. Learning how officers search buildings and make arrests gave the non-law enforcement members of CACIE an appreciation for what police are up against when dealing with violent gang members. It also underscored the fact that the fight against transnational gangs—regardless of one's nationality—can only succeed through a unified effort.

"The hope is that after this training, the participants will take an elevated role against gangs in their communities," Baer said, "and share with each other what works and what doesn't work."

"It's good to know there are so many other people in different countries committed to keeping kids out of gangs," said CACIE class member Fredy Martinez, a mental health therapist and court liaison with Arlington, Virginia's Department of Human Services who counsels young gang members caught up in the legal system. "This group—and what they stand for—validates what I do on a daily basis."

CACIE participant Henry Pacheco, a counselor for the Northern Virginia Family Service's Intervention, Prevention, and Education Program, acknowledged that the gang problem can sometimes seem overwhelming. "But there is hope," he said. "Just take a look at the people in this group. They all care, and they are all working together to make their communities better."

Part 3: Overcoming the Language Barrier (page 57)

The Transnational Gang Threat

Part 3: Overcoming the Language Barrier

For some Central American and U.S. participants in an FBI-led training program to combat the threat of transnational gangs, there may have been a considerable language barrier if not for the Bureau interpreters on hand to provide a verbal lifeline.

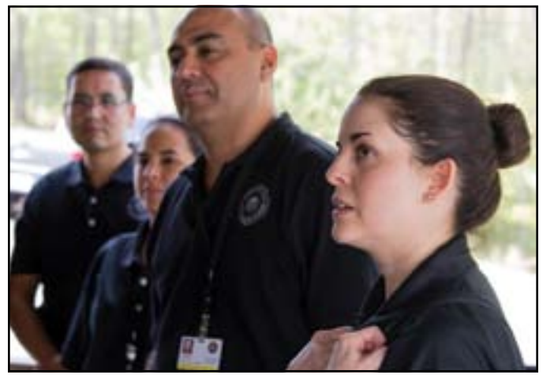
Although not technically members of the Central American Community Impact Exchange (CACIE) program, the four interpreters from our Language Services Section who recently took part in the two-week session were instrumental to the group's success, ensuring that the police officers, pastors, social workers, and community activists from Honduras, Guatemala, El Salvador, Belize, Costa Rica, Panama, and the U.S. were all on the same page.

A fundamental goal of CACIE is to facilitate an international coalition between law enforcement and communities to fight violent transnational gangs like MS-13 and 18th Street. The ability for partners from different countries to communicate—to share information and ideas—is central to that goal.

During presentations, participants who were not bilingual wore headsets to listen to an interpreter translating between English and Spanish. In the field, the linguists—whose regular assignments support a variety of FBI investigations—kept the dialogue flowing while the group toured neighborhoods and police stations in North Carolina and Guatemala learning about programs designed to keep young people out of gangs.

"What set this apart from our usual work is that it involved community leaders as well as law enforcement," said Ana Lahr, a linguist in our Pittsburgh Division who, like the other CACIE interpreters, volunteered for this assignment. "We had the privilege of interacting with all the participants and listening to their unique perspectives," she explained. "Everyone was passionate about the work they do."

Typically, interpreters try to be "invisible" and simply convey the speaker's message, said Martha Anta, a linguist in our San Antonio Field Office. But hearing about the challenges CACIE participants face in their



Martha Anta (right), a linguist in our San Antonio Field Office, interprets for the Spanish-speaking CACIE participants who did not speak English.

communities drew them all closer, she added. "It was extremely gratifying to be part of such a heartfelt group."

The linguists were never really off-duty. Training days sometimes stretched beyond 12 hours, and their interpreting skills were also needed for after-hours tours and meals. As a result, said Lillian Atdjian, a language specialist in our Jacksonville Division, "we became members of the group."

Thanks to the interpreters' efforts, noted CACIE participant Nick Hullinger, "the whole group was able to quickly move forward together. Their abilities made it easy for everyone to communicate and to bond." Hullinger, a Spartanburg (South Carolina) County Sheriff's Office deputy and member of an FBI Safe Streets Task Force, added that the language barrier posed little problem for the group.

There were emotional moments when it was difficult to interpret, said Sabrina Jennings, a language analyst in our Houston Field Office. During a meeting with at-risk youth in Durham, North Carolina, for example, a young boy talked about not having a father or father figure in his life. "As a male counselor told the young boy to stand up and proceeded to hug him, I found it difficult to maintain my composure as I watched people in the audience crying," Jennings recalled. "I kept interpreting with watery eyes and a lump in my throat."

Just like the CACIE participants, she added, "the interpreters don't simply walk away from an assignment like this. We all spent two weeks together, shared so much, and learned from each other. We all became friends."

Part 4: Adding Prevention to Intervention (page 58)

Left: CACIE participant Luis Ramirez, a National Civilian Police officer in Guatemala, said his department has placed a new emphasis on community-based policing. "We want to change the culture in these dangerous neighborhoods."

The Transnational Gang Threat

Part 4: Adding Prevention to Intervention

In an impoverished neighborhood in Guatemala known for its violent gang activity, a handful of youngsters show visitors around a small compound next to a playground and soccer field. Although the buildings have dirt floors and few amenities, they represent a future for these children—one designed to keep them beyond the reaches of gangs.

Mentors hired by the community help the youths with their studies there, encourage them to stay in school, teach them how to plant and cultivate a garden, and remind them of the dangers associated with gangs such as MS-13 and 18th Street.

Most of the children live with those dangers on a daily basis. Gang crime is severe in Guatemala. An average of nearly 16 homicides occur daily in the country, and most of them are gang-related. "My goal is to stay in school and one day become an auto mechanic," one of the boys in the program said. "With gangs, there is no future."

The youth program in the impoverished outskirts of Villa Nueva—Guatemala's second largest city—is called Project Hope and is an example of how communities are working to fight the gang threat through prevention as well as police intervention. That deterrence approach—keeping young people from being recruited by gangs—is a fundamental goal of the Central American Community Impact Exchange (CACIE) program, an FBI-led initiative.

CACIE recently conducted a training class for law enforcement and community leaders from six Central American countries and the U.S. aimed at exposing participants to community-based prevention programs that work so they might be implemented in other places.

"We want to change the culture in these dangerous neighborhoods," said Luis Ramirez, a National Civilian Police officer in Guatemala. His department has placed a new emphasis on community-based policing, recently launching a 14-month training program in which graduating officers will have the equivalent of a master's degree in community policing.

"We are constantly working on strategies to investigate the gangs and to stop the threat," Ramirez said. "Community programs to keep kids from joining gangs are one more strategy. We need to pay more attention to these at-risk kids."

In Guatemala and elsewhere in Central America, many teens don't go to school and don't work. Often, they come from broken homes, their parents are not around, and they are unsupervised. "The goal is to keep these youths from being idle," Ramirez said, "and to give them hope for the future." But resources to create and fund after-school and other programs like Project Hope are often in scarce supply in Central American countries like Guatemala.

"These are very challenging circumstances," Ramirez acknowledged. But a unified effort can make a difference, as CACIE participants saw in Villa Nueva and in Durham, North Carolina. "We all work together—the church, private enterprise, and the state," Ramirez said. "Individually, we might not have resources, but everyone can bring something to the table. Communities are made by everyone."

"We hope this year's CACIE class will take the best of what they learned and implement similar programs in their own communities," said Special Agent Rich Baer, who helps administer the program. "Because of the strong bonds they formed during the program, we are confident they will be good resources for each other going forward."

Latent Hit of the Year Award

Massachusetts Examiner Honored

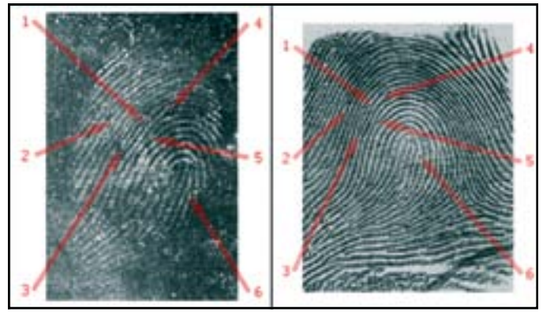
Every year, our Criminal Justice Information Services Division gives its Latent Hit of the Year Award to latent print examiners and/or law enforcement officers who solve a major violent crime using the Bureau's Integrated Automated Fingerprint Identification System, or IAFIS.

This year, we honor Massachusetts State Police (MSP) Trooper Christopher Dolan, a latent print examiner in the MSP's Crime Scene Services Section, for the role he played in identifying the killer in a 1983 cold case.

The victim, 29-year-old Rodney Wyman, and a co-worker had traveled from Connecticut to Malden, Massachusetts, to install windows at a construction site in the summer of 1983. On the night of August 22, the two men settled down in their motel suite to watch television. They heard a noise in a back room, and Wyman got up to check it out. As he approached the door, a gunman fired a fatal shot into Wyman's chest. The gunman, demanding money from Wyman's co-worker, brutally attacked the man and then began removing valuables from the room. But when he tried lifting the television set, a tamper alarm was activated, and two hotel employees rushed to the room. One of the employees saw a man exit the rear window of the suite and chased him, but the intruder escaped.

The motel room was processed by the MSP's Crime Scene Services Section. More than 23 latent prints were recovered—several were deemed of no value, and others were identified as those of the deceased victim and employees of the hotel. The remaining prints were searched against the Massachusetts Automated Fingerprint Identification System (AFIS), which was relatively new at the time. There were no results produced, and eventually, the case went cold

But 27 years later, the MSP—looking to apply newer investigative technologies to cold cases—requested a reassessment of the latent evidence from the Wyman homicide investigation. That task fell to Dolan, who first searched two latent images collected from the television set against the state AFIS, with negative results. He then requested a search of the FBI's IAFIS and, in less than 10 minutes, received a response containing possible



The latent print on the left was taken from a television set found at a crime scene in Malden, Massachusetts, in 1983. The fingerprint on the right from IAFIS was matched to the latent print by an examiner with the Massachusetts State Police.

candidates for comparison purposes. Dolan examined the evidence and positively identified the prints to the first candidate in the IAFIS response—Shawn Marsh.

Based on this identification, the MSP reopened the case. Investigators located Marsh and requested additional prints from him, which resulted in an additional match to palmprint evidence recovered from the crime scene. Marsh was indicted in September 2011, pled guilty in April 2013, and was sentenced to a lengthy prison term.

It turned out that some of Marsh's fingerprints had been available in the state AFIS at the time of the murder. However, the database was fairly new to the MSP, and those processing crime scene evidence at that time considered the prints of the right and left little fingers of limited value, so it was common practice to exclude them from the overall AFIS database in order to conserve resources. Why is that an important fact? Because the original latent prints lifted from the television set in the motel room crime scene came from a left little finger.

The full set of Marsh's fingerprints contained in IAFIS—which ultimately led to his identification—came from another arrest.

But the lesson was learned, and today, the Massachusetts State Police train law enforcement officers to collect prints from all 10 fingers when processing suspects.

Violation of Public Trust

Corrupt Officials Jailed for Abusing Justice System

In the run-up to the 2012 primary elections in Mingo County, West Virginia, a group of officials adopted a campaign slogan to promote their political slate: Team Mingo. But the judge, sheriff, and county prosecuting attorney who were part of the alliance—among the most powerful men in the local judicial system—used their authority to serve their own interests rather than those of the citizens who elected them.

"These men essentially ran the county's legal system," said Special Agent Jim Lafferty, who investigated the case out of our Pittsburgh Field Office. The ringleader was Circuit Court Judge Michael Thornsbury. "The judge and his team were the power in Mingo County," Lafferty explained. "They didn't like anyone who tried to oppose them. If you were an attorney or an individual who wanted to get a fair shake in the court system, you had to play whatever game they wanted you to play. It was a toxic environment."

We opened a case in September 2012. Lafferty and retired Special Agent Joe Ciccarelli—with the help of West Virginia State Police investigators—uncovered evidence that Thornsbury, then-Sheriff Eugene Crum (who had formerly been the county's chief magistrate judge), and Michael Sparks, then the county's prosecuting attorney, had been engaging in corrupt activities.

Specifically, the judge coerced a local drug defendant into firing his defense counsel because Thornsbury and other Team Mingo officials, including former County Commissioner David Baisden, learned that the drug defendant was prepared to testify that Sheriff Crum had illegally received prescription pain medication and obtained unlawful campaign contributions. To protect Crum, Thornsbury and his colleagues pressured the defendant into firing his defense attorney and replacing him with another attorney handpicked by Team Mingo. After switching lawyers and pleading guilty to lesser charges, the defendant dropped his allegations against Crum and was sentenced to up to 15 years in prison.

In addition, Thornsbury was later charged with trying to frame the husband of a woman with whom he was having an affair. The judge tried to have drugs planted in the husband's car. When that plan failed, he arranged to have the man arrested for stealing scrap metal—even when it was determined the man had been given permission to take the material.

In June, Thornsbury was sent to prison for more than four years for denying residents their constitutional rights. The federal judge who sentenced him compared Thornsbury's abuses of office to the actions of a Third World dictator.

Sparks, the former prosecutor who later cooperated with our investigation, was recently sentenced to a year in prison for his role in Team Mingo's illegal activities. Others previously jailed as a result of the corruption probe include Baisden, sentenced in January to 20 months' imprisonment, and former Mingo County chief magistrate Dallas Toler, sentenced in March to 27 months in prison.

"Team Mingo controlled the legal system, and they may have thought no one would stand up against them," said Lafferty, who has been investigating public corruption and white-collar crime for more than a decade. "That didn't turn out to be the case. No matter how much power you wield," he added, "when you violate the public trust and engage in corruption, sooner or later, you will get caught."

Serial Killers

Part 7: The FBI and Jeffrey Dahmer

At about 11:30 on the night of July 22, 1991, Milwaukee Police Department patrol units saw a partially clothed man stumbling down the road near an apartment building on North 25th Street. A handcuff could be seen dangling from his wrist. The young man reported to police that he had been threatened with a knife inside that apartment building, prompting the officers to investigate. And the first report on the incident to FBI Headquarters indicated that the police arrested a man named Jeffrey Dahmer at his apartment, where they had discovered what could have been the set of a horror movie—numerous body parts belonging to multiple victims.

In serial murder cases, the FBI's role is often that of providing forensic and other investigative support in an ongoing investigation. That was certainly the case with Dahmer.

After analyzing our options regarding jurisdiction in this case under the federal kidnapping statute, the Bureau offered its laboratory and identification services to local authorities in Milwaukee. To help identify previous victims, investigators began tracing the killer's trail across the U.S. and around the world. Behavioral analysts, also known as profilers, participated as well.

The remains of 11 victims were found in Dahmer's apartment. Evidence recovered there—from physical remains to tools used to torture and dismember victims—was sent to FBI Headquarters for forensic analysis. The Bureau ran DNA profiles; conducted chemical, biological, and tool mark analyses; undertook photographic and computer examinations; and performed other tests on submitted evidence. Bureau agents and analysts also investigated whether Dahmer could be linked to unsolved murders in areas where he was known to have lived, including Ohio, Florida, and Germany—one of the locations Dahmer was stationed while in the U.S. Army.

Soon after his arrest, Dahmer confessed to committing more than a dozen murders that included the torture and mutilation of his victims and the abuse of their corpses.

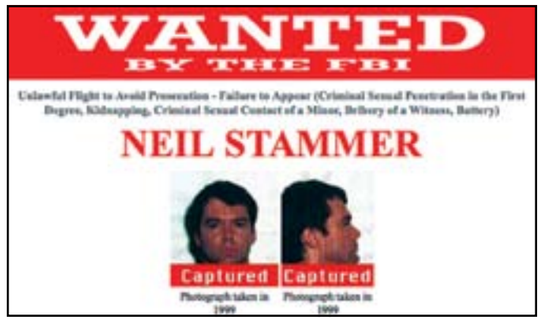
In early 1992, Wisconsin prosecutors—armed with evidence provided by the Bureau— began to set forth charges that Dahmer had killed 15 men during the course of a long criminal career. He was sentenced to life in prison and extradited to Ohio, where he was convicted of another murder. In 1994, while serving his sentence in a Wisconsin prison, Dahmer was bludgeoned to death by a fellow inmate.

In this 1991 handout from the Milwaukee County Sheriff's Department, serial killer Jeffrey Dahmer is seen in his mugshot. (AP Photo)

The FBI's involvement in serial killer cases has evolved over time. In the 1970s, we began applying the insights of psychology and behavioral science to violent criminal behavior. Federal legislation on serial killings in 1988 and on violent crimes against interstate travelers in 1994 expanded our operational jurisdiction. And of course, advancements in forensics over the years—such as DNA analysis and automated fingerprint capabilities—have played, and will continue to play, a vital role in stopping these killers and identifying their victims.

More about the Bureau's role in this case can be found on the FBI Vault, where we have made our Freedom of Information Act release of material on Dahmer available. This material was released a number of years ago and includes our Headquarters file, Milwaukee Division file, a file from the FBI Laboratory concerning tests made on evidence from Dahmer's apartment, and a foreign police cooperation file on efforts to determine if Dahmer had killed anyone while living in Germany.

Part 8: New Research Aims to Help Investigators Solve Cases (page 79)



Long-Time Fugitive Captured

Juggler Was on the Run for 14 Years

How do you catch a fugitive who has been on the run for 14 years, has traveled extensively overseas, speaks a dozen languages, and could be anywhere in the world?

The answer to that question, as Special Agent Russ Wilson learned, is a lot of hard work—and a little bit of luck.

Neil Stammer, a talented juggler with an international reputation, was recently arrested in Nepal and returned to New Mexico to face child sex abuse charges. The events that led to his capture are a testament to good investigative work and strong partnerships, and also to the strength of the FBI's fugitive publicity program.

Here's how the case unfolded:

Stammer, who once owned a New Mexico magic shop, was arrested in 1999 on multiple state charges including child sex abuse and kidnapping. He was released on bond but never showed up for his arraignment. New Mexico issued a state arrest warrant in May 2000; a federal fugitive charge was filed a month later, which allowed the FBI to become involved in the case.

Stammer, who was 32 years old when he went on the run, told investigators that he began juggling as a teenager to make money, and he was good at it. Before his 1999 arrest, he had lived in Europe as a street performer and had learned a variety of languages. At the time of his disappearance, it was reported that Stammer could read or speak about a dozen of them.

Given his overseas travel experience and his language skills, the juggler could have been hiding anywhere in the world. With few credible leads, the case against Stammer went cold.

Fast forward to January 2014. Special Agent Russ Wilson had just been assigned the job of fugitive coordinator in our Albuquerque Division—the person responsible for helping to catch the region's bank robbers, murderers, sex offenders, and other criminals who had fled rather than face the charges against them.

"In addition to the current fugitives, I had a stack of old cases," Wilson said, "and Stammer's stood out." Working with our Office of Public Affairs, a new wanted poster for Stammer was posted on FBI.gov in hopes of generating tips.

At about the same time, a special agent with the Diplomatic Security Service (DSS)—a branch of the U.S. Department of State whose mission includes protecting U.S. Embassies and maintaining the integrity of U.S. visa and passport travel documents—was testing new facial recognition software designed to uncover passport fraud. On a whim, the agent decided to use the software on FBI wanted posters. When he came upon Stammer's poster online, a curious thing happened: Stammer's face matched a person whose passport photo carried a different name.

Suspecting fraud, the agent contacted the Bureau. The tip soon led Wilson to Nepal, where Stammer was living under the name Kevin Hodges and regularly visiting the U.S. Embassy there to renew his tourist visa.

"He was very comfortable in Nepal," Wilson said. "My impression was that he never thought he would be discovered." Stammer had been living in Nepal for years, teaching English and other languages to students hoping to gain entrance into U.S. universities.

Although Nepal and the U.S. have no formal extradition agreement, the Nepalese government cooperated with our efforts to bring Stammer to justice. "We had tremendous assistance from DSS, the State Department, and the government of Nepal," Wilson said. "It was a huge team effort with a great outcome."

Health Care Fraud Enterprise Dismantled

Ringleader Operated Multiple Pharmacies

It was a combination health care fraud and drug distribution scheme on a massive scale. It involved 26 Michigan pharmacies, nine doctors, and two health care agencies. There were bribes and kickbacks aplenty and thousands of illegal doses of sought-after drugs like oxycodone and hydrocodone. And fraudulent billings to Medicare and Medicaid totaled more than $60 million, not to mention additional amounts to private insurers.

But the case began on a much smaller scale. In 2008, the Bureau learned that a single Michigan pharmacy was allegedly sending phony bills to Medicare and private insurance companies for prescription drugs. During the ensuing joint investigation with the Drug Enforcement Administration and the Department of Health and Human Services' Office of Inspector General, however, we were able to connect a wide array of other pharmacies—and subjects—to this illegal activity. We also uncovered the illegal diversion of controlled substances to people who didn't medically need them, as well as billings to the government and private insurers for millions of dollars of non-controlled medications that were never dispensed to patients.

In August 2011 and March 2013, a total of 39 individuals—including ringleader Babubhai Patel—were indicted on various federal health care fraud and drug charges related to this scheme, which ran from 2006 to 2011.

After a six-week trial, Patel was convicted and sentenced to a 17-year prison term in 2013. And just last month, the 38th defendant in the case was convicted in federal court. These defendants included pharmacists, doctors, home health care agency owners, an accountant, and a psychologist. (The 39th defendant is currently a fugitive believed to be outside the U.S.—law enforcement continues to pursue him.)

How the scheme worked. Patel, a pharmacist and businessman from Canton, Michigan, owned and/or controlled 26 pharmacies and several home health care agencies in that state, but he concealed his involvement in many of these facilities through the use of straw owners. He and his associates recruited a number

Care For You Pharmacy was one of the 26 Michigan pharmacies owned and/or operated by Babubhai Patel, who ran a criminal enterprise involved in health care fraud and drug diversion.

of pharmacists—mostly from overseas—to staff his pharmacies and help facilitate his scheme to defraud government and private insurers.

Patel and his associates offered kickbacks and bribes to doctors willing to write medically unnecessary prescriptions, home health care referrals, and bills for other services to Medicare, Medicaid, and private insurers. He also provided kickbacks and bribes to patient recruiters—individuals hired to go out and find patients willing to share their insurance information—as well as other inducements, such as doses of the drugs from the illegally written prescriptions. Patient recruiters, in turn, would then offer some of the same inducements to government and private insurance patients to get the patients to fill their prescriptions at Patel-owned pharmacies.

Such an extensive and complex fraud scheme required a similar response from law enforcement, and we obliged with the same sophisticated investigative techniques we've been using for years against savvy fraudsters—careful reviews of financial records, interviews, physical surveillance, undercover scenarios, confidential sources, court-authorized wiretaps, and analysis of medical data and corporate filings.

When all was said and done, a prolific criminal enterprise was completely dismantled. And its ringleader discovered that crime really doesn't pay: In addition to his 17-year prison sentence, Babubhai Patel was ordered to pay nearly $19 million in restitution to the insurance programs he had bilked.

Counterfeit Goods Smuggling Ring Dismantled

Undercover Agents Infiltrated Massive International Operation

When Ning Guo was sentenced to prison earlier this year, it marked one of the final chapters in a massive international counterfeit goods smuggling case in which criminals attempted to flood the U.S. market with bogus cigarettes, handbags, and sneakers from China that would have been worth $300 million on the retail market.

From November 2009 through February 2012, the smugglers and their conspirators attempted to import hundreds of shipping containers full of counterfeit Nike shoes, Gucci handbags, cigarettes, and other items from China into the U.S. through the Port Newark-Elizabeth Marine Terminal in New Jersey.

When a multi-agency force took down the operation in 2012, nearly 30 individuals were arrested and charged with various counts of conspiracy to traffic in counterfeit goods, as well as other crimes—including money laundering and drug trafficking.

"This was a complex case," said Special Agent Ron Pascale, who worked the investigation from our Newark Division. "But over time, we identified the entire conspiracy and dismantled it."

In 2008, our sources overseas identified a Chinese subject who wanted to smuggle counterfeit goods into the U.S. from China. That individual was introduced to an FBI undercover agent posing as a person at the port who had connections and could clear containers through

Left: Boxes containing some of the counterfeit goods seized during the investigation of a massive smuggling ring.

customs. Later, when the smuggler shipped a container of counterfeit cigarettes and learned that his U.S. buyer had fallen through, he asked our undercover agent to sell it for him—and he gave the agent a list of potential buyers.

With that list, Pascale said, the investigation expanded significantly—and soon led to Ning Guo, who bragged that he was the best person in the New York region to store and distribute counterfeit merchandise.

Using a variety of undercover operatives and working with other law enforcement partners—including U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection—the conspiracy was unraveled:

- Using false paperwork, the counterfeit merchandise was shipped in containers fraudulently associated with legitimate importers.
- Others in the ring managed the distribution of the goods once they were safely in the U.S. and cleared through the port.
- The merchandise was delivered to warehouses and distributed throughout New York, New Jersey, and elsewhere. Some of the conspirators paid hundreds of thousands of dollars to our undercover agents, whom they believed were assisting them.
- Some conspirators acted as wholesalers for the counterfeit goods, supplying retailers who sold the merchandise.
- Other conspirators took the profits and wired the money back to China.

In addition to undercover operatives, investigators used court-authorized wiretaps and sophisticated surveillance techniques to gather evidence. "We had the bad guys incriminating themselves in their own words," Pascale said, "and it was usually on tape and video."

The smuggling investigation also uncovered a scheme to import 50 kilograms of crystal meth into the U.S. "Counterfeiting always seems to be the gateway into something else," Pascale explained. "If these guys think they can get counterfeit shoes into the country, pretty soon they think they can get anything in."

He added, "Counterfeiting is never going to stop, so there will always be a reason to smuggle. That's why we will never stop working these cases."

FBI Files

CJIS Digitizes Millions of Files in Modernization Push

The era of sliding drawers full of aging FBI files is drawing to a close. Millions of fingerprint cards, criminal history folders, and civil identity files that once filled rows upon rows of cabinets—and expansive warehouses—have been methodically converted into ones and zeroes.

The digital conversion of more than 30 million records—and as many as 83 million fingerprint cards—comes as the FBI fully activates its Next Generation Identification (NGI) system, a state-of-the-art digital platform of biometric and other types of identity information. The system, which is incrementally replacing the Bureau's Integrated Automated Fingerprint Identification System, or IAFIS, will better serve our most prolific customers—law enforcement agencies checking criminal histories and fingerprints, veterans, government employees, and the FBI's own Laboratory.

The conversion from manual to digital systems began more than two decades ago, when paper files outgrew the space at FBI Headquarters in Washington, D.C. They were shipped to West Virginia, where the FBI built a campus in Clarksburg in 1992 for its Criminal Justice Information Services (CJIS) Division and leased warehouse space in nearby Fairmont for the burgeoning files. In 2010, CJIS broke ground on a new Biometric Technology Center and redoubled its efforts to digitize all the files. The most recent push—digitization of 8.8 million files in two years—not only added more data points to the NGI program, but also eliminated the need to move scores of cabinets full of paper into the new technology center.

"It makes those records immediately accessible to law enforcement across the country," said Penny Harker, who runs the Biometric Services Unit at CJIS. She said fulfilling requests for fingerprint matches—which once took hours—now takes just minutes or seconds. "It's a great benefit to them not having a delay simply because we were still storing files in a manual format."

The FBI's role as steward of so many identity files dates back to the 1920s, when the Bureau received 800,000 files from the U.S. Army. In the 1930s, the Bureau's Identification Division compiled the largest-ever collection of fingerprints from files collected from partner law enforcement agencies.

Rows of file cabinets in FBI facilities in West Virginia have been rendered obsolete in the FBI's effort to digitize decades of fingerprint cards, criminal history folders, and civil files.

The files that comprised the bulk of the digital conversion fell within three broad categories: criminal history files dating back to the early 1970s and before; civil identity files of people born prior to 1960 who enlisted in the military or applied for a government job; and fingerprint index cards. Files are maintained until individuals are 110 years old or dead.

After scanning and digitization, the paper files are destroyed, though original versions of historic files—fingerprint cards for John Dillinger, Bonnie Parker, and Clyde Barrow, to name a few—have been saved from the shredder.

"This is a monumental leap for us, because now we're not taking months to get back with a positive identification, said Jeremy Wiltz, deputy assistant director at CJIS. "With our Next Generation Identification, we're going to take that into seconds and sub-seconds."

NGI is scheduled to be fully operational in September. The digital conversion effort is also projected to be completed next month.

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

Left: This $80,000 boat owned by California con man David Rose was seized after law enforcement determined he had purchased it using funds he stole from his investors.

Investment Con Man Pleads Guilty

Fraudster Targeted Medical Professionals

It's an age-old scam: A smooth-talking individual offers an amazing investment opportunity—with promises of large returns—that turns out to be completely bogus. But because there are always people willing to accept these kinds of claims at face value and hand over their hard-earned money, it's a scam that continues to be effective.

Consider a recent case in Orange County, California, where just-convicted David Rose duped more than 75 doctors and dentists from around the country into shelling out more than two million dollars for him to invest in companies involved in researching and developing emerging medical technologies. But the investment money, despite what he promised, never made it any further than Rose's own bank accounts.

From at least March 2005 to around May 2011, Rose solicited mainly doctors to invest money with him through his company, M.D. Venture Partners. In many instances, he recruited investors by placing ads in medical publications, but he also got additional business through referrals from doctors who had already signed with him.

In his promotional material and in conversations and e-mails with prospective clients, Rose claimed that investor funds would be pooled and used to invest in companies developing new medical technology—an area that of course was of great interest to physicians. Rose even prepared for each client a private placement memorandum (PPM), a document commonly used in investments that fully lays out how invested funds will be used and what the risks are. The PPM also stated that Rose would receive a 2.5 percent "management fee."

To keep his clients engaged in the scam, Rose periodically consulted with them to solicit their medical expertise and bounce ideas off them. But they never saw any return on their investment.

In 2011, he began another scam, this one involving recruiting dentists and orthodontists into giving money to his new company, Technology Innovation Partners. He claimed that their funds would be pooled and invested in a company developing technology that would remove wisdom teeth in children without surgery. Like his previous scam, Rose targeted a certain group of people and relied heavily on referrals. He tapped into the medical expertise of his investors to keep stringing them along. He also prepared phony PPMs for his clients—only this time, he upped his "management fee" to 10 percent.

But by 2013, after several complaints to the FBI from his victims—the Bureau began investigating Rose and his investment activities. And through numerous interviews with victims and other witnesses and detailed examinations of Rose's financial records—tracking where the money actually went—we were able to gather enough evidence for a federal indictment against him.

Where did investors' money end up? Investigators found that Rose used it to rent pricey homes in California and purchase an $80,000 powerboat, luxury vehicles, expensive jewelry, college tuitions, and even shares of stock in a professional football team.

If you are contemplating investing your hard-earned money, here are a few tips to help you do it as safely as possible:

- 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 investment opportunities that offer unusually high yields.
- Check with a trusted financial adviser, broker, or attorney about any investments you are considering.

Corruption in a Small Texas Town

Investigation Dismantles Family-Run Criminal Operation

Public corruption arrests and convictions in major metropolitan areas usually garner a great deal of national attention. But big cities don't have a monopoly on crooked politicians—they can be found anywhere.

Like Progreso, Texas, a small town a few miles north of the U.S.-Mexico border. For almost a decade—from 2004 to 2013—several members of the same family, all Progreso government officials, used their positions to exact bribes and kickbacks from city and school district service providers. Through their illegal activities, they distorted the contract playing field, cheated the very citizens they purported to serve, stole education money from the children whose educations they were supposed to ensure, and lined their own pockets in the process.

Until the FBI got wind of what was going on, that is, and opened a case. Our investigation—which included confidential sources, undercover scenarios, financial record examinations, and witness interviews—collected plenty of evidence of wrongdoing and ultimately led to guilty pleas by the defendants. And on August 11, 2014, they were all sentenced to federal prison terms.

Jose Vela, the patriarch of the Vela family and leader of the corruption scheme, served as maintenance and transportation director for the Progreso Independent School District (PISD), which from 2004 to 2013 received more than a million dollars per year in federal program grants and funds from the U.S. Department of Education. But Vela's scope of influence was much broader than his job title suggested, thanks in part to the positions of his sons—Progreso Mayor Omar Vela and Michael Vela, president of the PISD Board of Trustees.

The elder Vela let it be known that contracts with the school district could be bought, and he accepted bribes

and kickbacks from contractors willing to pay. Jose Vela maintained control over the PISD and its board of trustees through a system of reward and retaliation: He distributed bribe money he received from contractors to trustees who voted as he directed; when trustees didn't vote with him, they were retaliated against—usually demoted, transferred, or ultimately forced out of their positions.

Vela's influence was not just over the PISD. With his sons' help, he took bribes and kickbacks from any entity—like construction companies and architectural firms—that wanted a public project contract with the city of Progreso. Vela, in effect, created a "pay to play" contracting environment in the city for such projects as municipal parks and libraries. He even extracted money from the lawyer who was supposed to be advising the school board.

Omar and Michael Vela assisted their father by collecting bribes from contractors and delivering the payments to him, keeping a portion for themselves.

A third Vela son was sentenced to a federal prison term as well for his role in a separate but related scheme. Orlando Vela, employed by the PISD as a risk manager, also headed a company purportedly in the business of supplying office products to school districts and admitted submitting thousands of dollars worth of phony invoices to the PISD for office supplies never received by the district.

And finally, also caught up in the overall corruption scheme was Jesus Bustos, who admitted to paying bribes and kickbacks to obtain contracts for his architectural firm. He was sentenced on August 27, 2014.

Public corruption at any level of government cannot be tolerated, and the FBI—uniquely situated to investigate it—will continue to address these allegations wherever we find them.

A Case of Corporate Greed

Executives Sentenced in $750 Million Fraud Scheme

Two former top executives of a publicly traded medical device company were sentenced to lengthy prison terms last week for their roles in a massive fraud scheme that cost shareholders $750 million.

Former ArthroCare Corporation Chief Executive Officer Michael Baker and Chief Financial Officer Michael Gluk were sentenced Friday to 20 years and 10 years in prison, respectively, for crimes including wire fraud and securities fraud. Two former vice presidents of the Austin, Texas-based company also received jail time.

"For years, the CEO and the CFO cooked the books to meet and exceed Wall Street's expectations," said Special Agent Duncan Edwards, one of several agents who worked the investigation out of our San Antonio Division. "It was only a matter of time before their crimes caught up to them."

Baker and Gluk were engaged in a sophisticated fraud scheme known in business circles as channel stuffing. "You get your distributors to buy more product than they need so the company's sales and revenue appear to be greater than they actually are," explained Special Agent Stephen Callender. "They were creating sales on paper that didn't exist in reality."

Beginning in 2005 and continuing until 2009, Baker orchestrated a series of end-of-quarter transactions involving distributors who willingly received more of ArthroCare's product—a specialized needle used in back surgeries known as a spine wand—than they expected to sell.

The distributors agreed to stock their shelves with the extra devices because ArthroCare made it profitable to do so. Distributors were given a fee for taking extra product or given generous terms to pay for the devices. Some were told they could return the spine wands at no cost if they didn't sell.

This long-running misrepresentation of sales gave ArthroCare the appearance of significant growth, and its stock price climbed—even as Baker lied to investors and analysts about ArthroCare's relationships with its distributors.

"The CEO was digging the company into a bigger and bigger hole to maintain the stock's inflated price," Callender said. At one point, the company bought one of its distributors in an effort to sidestep regulatory reporting requirements.

But the fraud was getting too big to control, and in July 2008, amid public speculation of the channel stuffing scheme, the company announced it would restate previously reported financial results as a result of an internal investigation. The price of ArthroCare shares plummeted, resulting in an immediate loss in shareholder value of more than $400 million, and total losses of more than $750 million.

"There were countless victims in this case," said Special Agent Robert Cochrane, "including individual investors, banks, and large investment funds."

The FBI opened a case in 2011. Over the next three years, investigators combed through tens of thousands of paper and electronic records and documents; they also crisscrossed the country interviewing distributors, investors, and other individuals. In June 2014, after a four-week trial in Texas, a federal jury convicted Baker and Gluk.

"This scheme of betrayal and deceit was carried out by the defendants without regard to the deep-reaching and irreparable harm their actions caused to thousands of victims," said Chris Combs, special agent in charge the San Antonio Division. "Many of the victims will never recover from the financial ruin caused by the defendants' greed."

Special Agent Tom Hetrick, another agent who worked on the investigation, noted that the lengthy prison terms given to the CEO and CFO should send a clear signal: "No matter what your title or position, no one is above the law. This type of corporate fraud is unacceptable."

Vintage Fraud

Rare Wine Dealer Sentenced in Counterfeiting Scheme

"The same old wine in a brand new bottle" is a phrase that aptly describes how fraudsters deceive the public in ever-changing ways. It applies perfectly to Rudy Kurniawan's profitable and long-running counterfeiting scam—except that Kurniawan was putting new wine in old bottles.

Earlier this month, a New York federal judge sentenced Kurniawan to a 10-year prison term for his elaborate counterfeiting scheme in which he mixed newer, cheaper wines together and poured them into old bottles with forged labels.

When FBI agents executed a search warrant at Kurniawan's California home in 2012, they found wine-making materials everywhere in plain sight. "Essentially, the entire house was a fake wine-making laboratory," said Special Agent Adam Roeser, who helped investigate the case out of our New York Division.

"There were old bottles soaking in the sink. There was fresh wax dripping off bottles in another room," Roeser said. "There were piles and piles of corks, and on the kitchen counter there were 30 to 50 open bottles with a funnel and re-corker next to them. We found fake labels going back to 1899. He could make any label going back to the end of the 1800s."

Investigators are not certain how long Kurniawan—an Indonesian citizen who was in the U.S. illegally—was engaged in his scheme, but he appeared on the wine scene a decade ago, buying rare wines and later selling them. With access to a seemingly endless cache of rare and expensive Burgundies and Bordeaux varieties, among others, he was the toast of the town among a small group of high-end dealers and collectors.

"Wine is a collectible just like art," said now-retired Special Agent Jim Wynne, a long-time member of the FBI's Art Crime Team who investigated the Kurniawan case. "People want this stuff. Kurniawan was able to establish a persona as a rare wine connoisseur, and everyone believed his story."

Kurniawan befriended auctioneers and private collectors. He picked up the tab at expensive wine dinners with big-name chefs in Los Angeles and New York. And through those connections, he sold approximately $30 million worth of counterfeit wine.

Fake vintner labels used by wine dealer Rudy Kurniawan in his massive counterfeiting scheme.

"People were seduced by him," Wynne said, "and many suspended their good sense. And these were not stupid people," he added. "The people who can pay tens of thousands of dollars for a bottle of wine are often extraordinarily successful and wealthy. They just took it on faith that Rudy was telling the truth."

Ultimately, French wine makers who became suspicious of Kurniawan's claims cooperated with investigators to help to stop the fraud. With their help and the "typical gumshoe work" of investigators interviewing people and reviewing countless records, Roeser said, Kurniawan was arrested in 2012 and found guilty by a jury at trial in December 2013.

"The evidence against Kurniawan was overwhelming," Wynne said. "He was the forger, consignor, and marketer, all in one."

Besides counterfeiting, Kurniawan was also found guilty of bank fraud relating to a $3 million loan he obtained by providing false information, including omitting more than $7 million in outstanding loans, misrepresenting his annual expenses, and claiming he was a permanent U.S. resident when he had no legal immigration status in the country.

In addition to the prison sentence, Kurniawan was ordered to forfeit $20 million and to pay more than $28 million in restitution to his victims.

Left: An FBI Laboratory-constructed house model is a replica of the building where the victims in a Cleveland labor trafficking case were held. Using the model, one of the victims and other witnesses were better able to describe what was going on in the house to investigators and to the jury during the defendants' trial.

Justice in Labor Trafficking Case

Subjects Get Lengthy Prison Terms

In October 2012, a young woman was arrested by police in Ashland, Ohio for shoplifting a candy bar. But when she explained why she stole the candy, her story concerned the officers, and, eventually—after additional information was obtained—the Cleveland FBI opened a federal investigation into the matter.

It turned out that the young woman, who was cognitively disabled, was being held against her will and forced to perform manual labor for a couple who lived in a multi-dwelling house not far from the store where she was arrested. And it wasn't just the woman herself being held—it was her young daughter as well. Mother and daughter had been living in the apartment—in squalid conditions and enduring constant threats—since August 2010. The withholding of food was just one of the methods their captors used to control them.

Last month, after an investigation by the FBI and the Ashland Police Department, a federal judge handed down substantial prison terms for the two primary defendants following their convictions on labor trafficking charges: Jordie Callahan was sentenced to 30 years, while Jessica Hunt received a 32-year sentence. And earlier this year, acquaintances Daniel Brown and Dezerah Silsby were also sentenced for their supportive roles in the conspiracy to deprive the victims in this case of their freedom.

Back in 2010, Callahan and Hunt, who knew about the young woman's disability, targeted her and her daughter and invited them to live in their apartment. Once there, the defendants used force, threats of force, physical restraint, and threats of physical restraint to make sure they stayed, forcing the older victim to clean and do yard work.

Some of the defendants' actions included:

- Forcing the victims to sleep on a cement floor in a locked basement, then on the floor in a locked bedroom;
- Keeping the younger victim locked in a bedroom while her mother worked and not allowing either victim to use a bathroom until all of the day's chores were completed;
- Giving the victims minimal food and water;
- Sending the woman to the store for food and other items and threatening to harm her daughter if she didn't return within a certain time frame;
- Taunting the victims with pit bulls and snakes;
- Forcing the woman to hit her daughter while her actions were recorded with a cell phone, then threatening to show the video to authorities if the woman didn't do their bidding; and
- Physically harming the woman by slamming a door on her hand or kicking her in the hips, then taking her to the emergency room and confiscating any prescription pain medicine she received to feed their own drug habits.

Fortunately, the October 2012 arrest of the woman for shoplifting ultimately led to her freedom—and the freedom of her daughter.

An integral aspect of the federal case against Callahan and his co-conspirators was the work done by the FBI's victim specialist in Cleveland and the U.S. Attorney's Office victim-witness coordinator, who jointly navigated through a myriad of organizations and government entities to ensure that both mother and child received needed services and support, from the beginning of the case through trial, sentencing, and beyond.

Money Laundering Takedown

Operation Targets Sinaloa Drug Cartel

In a major takedown in Los Angeles on Wednesday, September 10, nearly 1,000 federal, state, and local law enforcement officers seized approximately $100 million in cash, arrested nine subjects, and searched dozens of businesses in the city's downtown fashion district alleged to have laundered money for Mexican drug cartels.

The ongoing investigation—three indictments were unsealed Wednesday—is specifically aimed at the Sinaloa Cartel and its activities, including narcotics trafficking, hostage taking, and money laundering in Los Angeles and elsewhere in the U.S. and Mexico.

In one case, the cartel used a fashion district business to funnel ransom payments related to a kidnapped U.S. citizen who was held hostage and tortured by cartel members in Mexico.

"The victim, who worked as a distributor for the Sinaloa Cartel, was kidnapped after 100 kilograms of cocaine he was supposed to distribute were seized by U.S. law enforcement," said Bill Lewis, assistant director in charge of our Los Angeles Field Office. The victim—who was ultimately released and safely returned to the U.S.—was kidnapped because of his drug debt.

The cartel sent demands to the victim's family in the U.S. and instructed them to deliver the ransom money—separate payments of $100,000 and $40,000—to a Los Angeles business known as QT Maternity. "Our investigation determined that the ransom payment was distributed to 17 other businesses located in the fashion district," Lewis said. "These stores were used as third-party money launderers in a scheme commonly referred to as the Black Market Peso Exchange."

The peso exchange scheme essentially turns dollars into Mexican currency through the sale of legitimate goods. The Mexican businesses that participated used illicit drug money to purchase goods, which were then sold in Mexico for pesos. The proceeds were returned to the cartel in Mexican currency. This laundering process avoided the risk of smuggling large amounts of cash across the border.

At one location during the September 10 takedown in Los Angeles, FBI agents seized nearly $3 million in cash.

"We have targeted money laundering activities in the fashion district based on a wealth of information that numerous businesses there are engaged in Black Market Peso Exchange schemes," said Central District of California Assistant U.S. Attorney Robert Dugdale. "Los Angeles has become the epicenter of narco-dollar money laundering, with couriers regularly bringing duffel bags and suitcases full of cash to many businesses. Because Los Angeles is at the forefront of this money laundering activity," he explained, "law enforcement in Los Angeles is now at the forefront of combating this issue."

Wednesday's operation was the result of a task force investigation made up of multiple federal and local law enforcement agencies, including the FBI, the Los Angeles Police Department, the Drug Enforcement Administration, the Internal Revenue Service, and U.S. Immigration and Customs Enforcement's Homeland Security Investigations. ICE-HSI efforts alone resulted in seizures of more than $65 million.

"Today's arrests and searches should send a message to international drug cartels that the FBI and our partners won't tolerate the exploitation of American businesses for the purposes of illicit financial transactions that fund hostage taking and the distribution of narcotics," Lewis said Wednesday after the takedown. "In addition, today's actions should send a warning to American businesses that turn a blind eye to the crime they facilitate while avoiding reporting requirements, transaction fees, and law enforcement scrutiny."

Murder-for-Hire Plot Uncovered

Subject Wanted Out of $8 Million Debt

It's a novel way to have your debt forgiven—hire a hit man to kill your creditor. However, it's also illegal. Just ask the Illinois businessman who recently received a federal prison term for attempting to arrange such a murder.

Daniel Dvorkin, a commercial real estate professional, had taken out business loans a number of years ago. When the economy took a downturn around 2008, Dvorkin's businesses took a hit, and he was unable to pay back those loans to the bank. Eventually, his loans were bought out by a Texas businessman and his company, which sued Dvorkin in civil court, winning an $8.2 million judgment against Dvorkin and two of his companies in February 2012.

On April 2, 2012, both sides sat down to mediation, trying to find some middle ground regarding the judgment and a dollar amount both parties could live with. But it failed.

Three days later, Dvorkin called an acquaintance and asked to meet the next day at Dvorkin's office in Oakbrook Terrace, a Chicago suburb. When this individual came to the office, Dvorkin walked him outside and asked for help with finding a hit man. Giving his acquaintance a copy of the judgment order and two Internet documents clearly identifying the intended victim as the Texas businessman, Dvorkin said he wanted his target to "stop breathing."

They discussed specifics: Dvorkin had $35,000 in untraceable cash saved and could come up with another $15,000 to pay upfront; he would then pay another $50,000 after the murder. He told his acquaintance he could arrange for a flight on a private jet so the hit man's name wouldn't appear on any commercial flight records. And he indicated that he would want to be out the country when the murder occurred so he wouldn't be a suspect.

Dvorkin also explained that he was currently appealing the judgment order and thought that if the Texas businessman did not or could not respond to the appeal, the funds wouldn't have to be paid out.

How do we know what Dvorkin said during this conversation? Because several days after it took place, the acquaintance contacted the Oakbrook Terrace Police Department and reported Dvorkin's attempt to solicit a murder. Oakbrook police then contacted the FBI's West Resident Agency—a satellite of our Chicago office—and our investigators reached out to the acquaintance, who readily agreed to consensually monitor any related future conversations with Dvorkin.

Over the next few weeks, and at the behest of law enforcement, the acquaintance-turned-cooperating witness called and met with Dvorkin several times, following up on their April 6 conversation and moving the plot ahead. But during a meeting on May 7, Dvorkin told our witness that he had hired another hit man—one who only charged somewhere in the $20,000 range and only needed a 10 percent down payment. The FBI, concerned by this turn of events, immediately contacted the intended victim in Texas and arranged for protection for him and his family. Investigators also approached Dvorkin that same day, letting him know they were aware of his murder-for-hire plot—without giving away the identity of the cooperating witness.

After further investigation and collection of additional evidence, Dvorkin was arrested on July 5, 2012. And in August 2013, after a five-day trial, a jury found him guilty—most likely due to Dvorkin's own incriminating words captured on court-authorized recordings.

Sweepstakes Fraud

Senior Citizens Targeted

A North Carolina couple recently pled guilty to running a sweepstakes fraud scheme that targeted elderly Americans, in some cases causing victims to lose their entire life savings.

Jessica and Jason Brown acknowledged in federal court that they operated call centers in Costa Rica that falsely informed U.S. residents—predominantly senior citizens—that they had won a substantial cash prize in a global sweepstakes, but the prize was only redeemable if the "winners" sent money to cover insurance and other fees. From 2004 until 2013, the Browns and their crew fleeced hundreds of elderly Americans out of nearly $900,000.

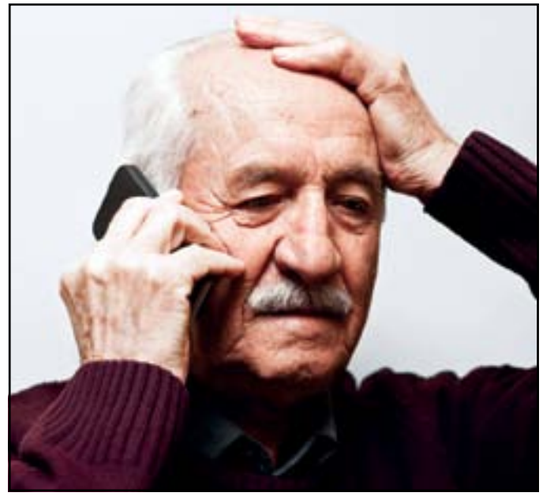
"They could make themselves extremely believable over the phone," said Special Agent Scott Duffey, who investigated the case from our Baltimore Division. "For people on the other end of the line who were even a little bit gullible or desperate for money, the deception could be too much to resist."

"The victims of these scams are not just people without an education," noted Pat Donley, a senior litigator with the Department of Justice who has prosecuted many sweepstakes fraud cases. "Some victims have been doctors, others Ph.Ds. They are just taken in."

Those who carry out these types of telemarketing frauds, including the Browns, use Internet technology and even forged documents to dupe their victims. They also purchase marketing lists—commonly used by lawful telemarketers—so they may know something about their victims, such as credit cards they might possess.

The fraudsters work out of so-called boiler rooms, usually apartments or offices with banks of phones. They might make hundreds of calls before finding one person receptive to their pitch. Typically, the criminals say they are calling on behalf of some reputable insurance company or a U.S. federal agency such as the Federal Trade Commission or the Internal Revenue Service. The imposters say they want to make sure all the taxes are paid on the sweepstakes money so the winner faces no legal or tax issues.

To mask that they were calling from Costa Rica, the Browns used readily available technology that made victims think they were talking to someone from an area code in Washington, D.C. This added a further air



of legitimacy to the scheme, since the callers frequently claimed to be representing a U.S. federal agency.

Though initial prizes were usually billed as second-place winnings, the $350,000 to $400,000 figures were still substantial. The victims were told they would have to pay fees and taxes of about 10 percent—between $3,500 and $4,000—and were often directed to send the money via Western Union.

It didn't stop there. After receiving money, the scammers would contact the victims again and inform them that their prize amount had increased, either because of a clerical error or because another prize winner was disqualified. Of course, the new, larger prize meant more taxes and fees. The attempts to collect more cash would continue until a victim either ran out of money or realized what was going on, Duffey explained. "One Delaware woman was swindled out of more than $300,000—her life savings," he added.

Donley has seen similar schemes ruin elderly victims financially. "One person in Florida gave up more than $800,000," he said, "and a woman from California gave up most of her savings that she was going to use to care for her two handicapped children. These criminals are heartless," he continued. "It's easy for them to rob people, because they never meet the victims and never see the consequences."

Left: The data center at the Criminal Justice Information Services Division in West Virginia is home to the Next Generation Identification System, or NGI.

Next Generation Identification

FBI Announces Biometrics Suite's Full Operational Capability

Agencies searching the FBI's criminal history record database for matches to their subjects are getting faster and more accurate responses—the result of the Bureau's 10-year effort to improve its ability to provide law enforcement partners with timely, high-quality identification.

Earlier this month, the FBI announced the Next Generation Identification system, or NGI, is now at full operational capability. The system replaced the Integrated Automated Fingerprint Identification System (IAFIS), the Bureau's longstanding repository for fingerprints. NGI's incremental roll-out, which began in 2010, has already seen significant improvements in accuracy rates on queries, the result of new high-tech tools and algorithms that more effectively search more than 100 million records. Fingerprint matches are now better than 99 percent accurate, and hits on latent prints (prints lifted from crime scenes, for example) have tripled from 27 percent accuracy in the old IAFIS system to more than 81 percent today.

"NGI gives us this opportunity to not only upgrade and enhance technology that we've been using for years, but it also lets us leverage new technology that can help us do our jobs better," said Steve Morris, assistant director of the FBI's Criminal Justice Information Services (CJIS) Division, which runs NGI.

Enhancements under NGI include the following:

- **Repository for Individuals of Special Concern (RISC):** Deployed in 2011, it's a searchable subset of what Morris described as the database's "worst of the worst offenders," including terrorists and dangerous fugitives. Using a mobile device, police can take two fingerprints from a subject and remotely query the database and get immediate results.
- **National Palm Print System:** In May 2013, NGI expanded beyond traditional finger and thumbprint capabilities to include palms. Morris said the majority of prints left at crime scenes contain hand ridges and palm prints.
- **Rap Back:** Entities that conduct background checks on individuals holding positions of trust (teachers, camp counselors) can receive notifications if the individual is subsequently involved in criminal activity. Launched earlier this year, Rap Back is named for the process of reporting back when a person is involved in criminal activity.
- **Interstate Photo System (IPS):** Launched this year, NGI's facial recognition capability provides a way to search millions of mug shots or images associated with criminal identities for potential matches. Note that civil files (such as those in Rap Back) and criminal mug shots reside in a repository separated by identity group, so an innocent schoolteacher's image isn't going to appear when the system returns an array of possible candidates in a criminal query.

In safeguarding privacy and protecting the public's rights and civil liberties, NGI is subject to the same extensive security protections, access limitations, and quality control standards already in existence for IAFIS. A thorough privacy impact assessment is completed and submitted to DOJ for each enhancement under NGI.

The facial recognition system is not connected to the Internet or social networks or your local Department of Motor Vehicles. "Facial recognition doesn't mean that we somehow now have this ability to go out and start collecting video feeds," Morris said. "That's not what this is about. It's a technology that allows us to digitally compare criminal mug shot photos that we have in our database against one another."

For more than 18,000 law enforcement agencies and partners—and their constituents—upgrading to NGI means increased accuracy and improved, faster intelligence.

FBI Releases Study on Active Shooter Incidents

Covers 2000-2013 Time Frame

Today the FBI is releasing a study of 160 active shooter incidents that occurred between 2000 and 2013 throughout the U.S. The primary purpose of the study? To provide our law enforcement partners—normally the first responders on the scene of these dangerous and fast-moving events—with data that will help them to better prepare for and respond to these incidents, saving more lives and keeping themselves safer in the process.

But we believe the information contained in this study can benefit anyone who could potentially be in an active shooter situation—like emergency personnel, employees of retail corporations and other businesses, educators and students, government and military personnel, members of the general public, etc.—by giving them a better understanding of how these incidents play out.

We began the study in early 2014. With assistance from Texas State University's Advanced Law Enforcement Rapid Response Training Center, we researched possible active shooter incidents in the U.S. during our selected time frame using official police records, after action reports, and shooting commission documents as well as FBI resources and open source information. We identified 160 events that fit our criteria—individuals actively engaged in killing or attempting to kill people in populated areas (excluding shootings related to gang or drug violence).

Once the incidents were identified—and we're confident that our research captured the vast majority of active shooter events falling within the specified time frame—we looked at each incident separately to identify its characteristics, then we correlated the data from all of the incidents to get a fuller picture of active shooter incidents in general.

Because so many of these incidents unfold so rapidly, Special Agent Katherine Schweit—who heads the FBI's Active Shooter Initiative—says she hopes the study "demonstrates the need not only for enhanced preparation on the part of law enforcement and other first responders, but also for civilians to be engaged in discussions and training on decisions they'd have to make in an active shooter situation."

Using the results of this study, the Bureau's behavioral analysis experts will now delve deeper into why these

The above graphic depicts the characteristics of the 160 active shooter incidents identified between 2000 and 2013 that were used in the study.

shooters did what they did in an effort to help strengthen prevention efforts around the country.

Today's study is just one of the resources the FBI offers to its law enforcement partners and others to help coordinate and enhance the response to active shooter incidents. Other resources—due in part to last year's Investigative Assistance for Violent Crimes Act and a federal multi-agency initiative targeting violent crime—include training for first responders, conferences for law enforcement executives, operational support in the event of an active shooter event, and assistance to victims. The Bureau is in a unique position to offer this type of assistance—we've played a large role in supporting the response to every major active shooter incident in recent years.

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

Help Us Catch the AK-47 Bandit

Violent Bank Robber Shot a Police Officer

During what authorities believe was his first bank robbery nearly three years ago in Chino, California, the AK-47 Bandit—so named because he carries an assault rifle during takeover-style robberies—shot and seriously wounded a police officer while making his escape. Since then, he has robbed or attempted to rob five more banks, most recently in August, when he hit a rural bank in Nebraska.

"He has shown he is not afraid to shoot someone, and experience tells us he is not going to stop robbing banks until we catch him," said Special Agent Kevin Boles, who is working the case out of our Los Angeles Field Office. "We feel like we are racing the clock on this guy," Boles said. "If we don't get him soon, things could end badly and someone else might get hurt."

That's why we are asking for the public's help and renewing our publicity campaign regarding this violent criminal. There is a reward of up to $100,000 for information leading to the arrest and conviction of the AK-47 Bandit.

Here is what we know:

- He is a white male, approximately 25 to 40 years old, about 6 feet tall, with light-colored eyes and a stocky build.
- During robberies he wears a dark balaclava ski mask, body armor, and black gloves.
- He carries an AK-47 assault rifle with a drum magazine.
- In several of the robberies, his getaway car was a dark gray four-door Nissan Maxima with chrome accents, model year 2009-2011.
- The robberies occurred on February 29, 2012, in Chino (California Bank & Trust); March 12, 2012, in Vacaville, California (Bank of the West); July 6, 2012, in North Bend, Washington (Chase Bank); November 7, 2012, in Rexburg, Idaho (East Idaho Credit Union); and August 22, 2014, in Nebraska City, Nebraska (First Nebraska Bank). There was also an attempted robbery on March 9, 2012, in Sacramento, California, at the Tri-Cities Bank.

Police believe the variety of surveillance video from the robberies—and a voice recording—may help the public identify this criminal. "We truly believe that someone knows this suspect, whether they are familiar with his physique, his voice, his vehicle, or even some of the apparel he's wearing during the robberies," said Bill Lewis, assistant director in charge of our Los Angeles Field Office during a 2013 press conference announcing the reward offer. "We are hoping citizens will take notice, look a little closer, and think a little harder about whether they have information that could break this case."

Anyone with information about the AK-47 Bandit's identity or whereabouts is urged to contact investigators at the toll-free number 1-800-CALL-FBI or send an e-mail to bandit@chinopd.org. Information can be provided confidentially.

Bank surveillance photographs of the vehicle and the suspect can be found at the Chino Police Department's website: http://www.chinopd.org. Additional bank surveillance photos and videos can be found on the FBI's wanted poster.

Billboard advertising has also been donated to assist with the publicity campaign. Digital ads, including bank surveillance images, the reward offer, and the toll-free number, are running in the Los Angeles region and other areas where robberies occurred. The FBI's social media channels are helping to publicize the case as well.

"This guy attempted to murder a police officer," Boles said. "There is no telling what he is capable of. We need to get him off the streets for everyone's safety."

Note: The AK-47 Bandit may have been located since the above information was posted on our website. Please check bankrobbers.fbi.gov for up-to-date information.

National Cyber Security Awareness Month

Security is Everyone's Responsibility

Every October since 2004, National Cyber Security Awareness Month—administered by the Department of Homeland Security (DHS)—reminds us of the importance of protecting not only our individual identities, finances, and privacy but also our country's national security, critical infrastructure, and economy. Cyber security is a responsibility shared by all—the public sector, the private sector, and the general public.

Individually, Americans should ensure the security of their own computers and other electronic devices. You don't want criminals accessing your bank accounts online. You don't want to become part of a criminal botnet responsible for stealing millions of dollars. You don't want to unknowingly infect your company's computer network with a damaging virus.

So how can you protect against those scenarios? Here are a few tips:

- Make sure you've got updated antivirus software installed;
- Enable automated patches for your operating system;
- Don't open e-mail attachments or click on URLs in unsolicited e-mails;
- Use strong passwords, and don't use the same one or two passwords for everything; and
- Avoid putting out personally identifiable information on social media platforms.

In other words, make it as difficult as possible for criminals and others to use your digital technology against you, against other innocent victims, and against our nation as a whole.

Agencies across the U.S. government, including the FBI, are making cyber security a top priority as well.

Within the Bureau, we prioritize high-level intrusions by the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. Collaborating with our partners—including DHS, the intelligence community, law enforcement at all levels, and the private sector—we strive to predict and prevent these kinds of intrusions, not just investigate them after the fact.

Our legal attaché offices coordinate international investigations and address jurisdictional hurdles and differences in the law from country to country, supporting and collaborating with newly established cyber crime centers at Interpol and Europol.

We work side by side with our federal, state, and local partners on cyber task forces in each of our 56 field offices and at the National Cyber Investigative Joint Task Force.

We also exchange information about cyber threats with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensic and Training Alliance.

So do all these partnerships make a difference? Here are some recent case examples that clearly demonstrate the value of collaboration:

- In August 2014, a Chinese national was indicted on charges stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors.
- In June 2014, a multinational effort disrupted the GameOver Zeus botnet, believed to have been responsible for the theft of millions of dollars from business and consumers in the U.S. and abroad.
- In May 2014, five hackers—members of China's People's Liberation Army—were indicted on charges of illegally penetrating the networks of six U.S. companies and stealing proprietary information, including trade secrets.
- Also in May 2014, the co-developers of a particularly insidious malware known as Blackshades—which is believed to have infected more than half a million computers around the world—were indicted.

Stay tuned to our website during the month of October for more information on cyber security, cyber threats, investigative activities, and wanted cyber fugitives.

Seeking Information

Help Identify Individuals Traveling Overseas for Combat

The FBI is asking for the public's help identifying individuals who have traveled—or are planning to travel—overseas to engage in combat alongside terrorist organizations.

"We need the public's assistance in identifying U.S. persons going to fight overseas with terrorist groups or who are returning home from fighting overseas," said Michael Steinbach, assistant director of the FBI's Counterterrorism Division.

The FBI is also seeking information about an English-speaking individual and others seen in a propaganda video released last month by the group calling itself the Islamic State of Iraq and the Levant, or ISIL.

In the video, a man whose face is obscured by a mask alternates seamlessly between English and Arabic in pro-ISIL pronouncements intended to appeal to a Western audience. Dressed in desert camouflage and wearing a shoulder holster, the masked man can be seen standing in front of purported prisoners as they dig their own graves and then later presiding over their executions.

The video was released on September 19. In releasing a segment from the video, the FBI hopes someone recognizes the man. In the segment, faces of purported prisoners are obscured and their executions are not shown.

The subject in the video has what is believed to be a North American accent. FBI Director James Comey has said about a dozen Americans are known to be fighting in Syria on the side of terrorists.

Left: A 55-minute ISIL propaganda video features an English-speaking man with what is believed to be a North American accent.

The threat of U.S. citizens traveling overseas to fight alongside terrorist groups is not new. Two years ago, a Chicago man was imprisoned for planning to travel to Somalia in 2010 to join al Shabaab. Last year, an Albanian man living in Brooklyn was sentenced to 15 years for attempting to travel to Pakistan to engage in violent jihad. Last month, a New York man pled guilty to attempting to travel to Yemen in 2012 to support al Qaeda. On Saturday, a Chicago man was arrested for allegedly attempting to travel overseas to join ISIL.

Earlier this year, the FBI's Minneapolis Division launched a campaign to raise awareness in communities and law enforcement circles about the foreign traveler threat. Minneapolis created a unique tip line and distributed business cards to community leaders asking for information about anyone who might be planning travel—or had already traveled—to a foreign country for armed combat.

"These homegrown violent extremists are troubled souls who are seeking meaning in some misguided way," Director Comey said during a recent *60 Minutes* interview. "And so they come across the propaganda and they become radicalized on their own independent study, and they're also able to equip themselves with training again on the Internet, and then engage in jihad after emerging from their basement."

ISIL has released several videos in recent months showing the beheadings of American, French, and English journalists and aid workers. The speaker—and executioner—in those videos has a British accent and authorities have said they now know his identity. The propaganda video highlighted today features a fluent English speaker and appears to be a stylized recruitment tool designed to lure Westerners to ISIL's cause.

The FBI needs your help identifying the individuals in this video as well as anyone traveling abroad to join terrorist organizations. Please send tips to www.fbi.gov/ISILtips or call 1-800-CALL-FBI (1-800-225-5324) with information.

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

Serial Killers

Part 8: New Research Aims to Help Investigators Solve Cases

Mention the term serial killer and what comes to mind for many people are murderers like Ted Bundy and John Wayne Gacy, whose grisly deeds seem to haunt our collective imagination.

But when Bob Morton considers serial killers—which he has spent much of his professional life doing—the recently retired special agent formerly with our Behavioral Analysis Unit thinks mostly about statistics.

Morton, the author of a new study on serial murder for the FBI's National Center for the Analysis of Violent Crime, spent the last eight years gathering and analyzing details from hundreds of serial murder cases to help investigators better understand these terrible crimes—and be better equipped to solve them.

"In the past," Morton said, "research tended to focus on known offenders and what led them to become serial murderers." That information, while useful, provided little help to investigators trying to apprehend an unknown offender in an active, unsolved case.

The new study—*Serial Murder: Pathways for Investigations*—focuses on a key aspect of serial murder cases: how and where the victims' bodies are discovered and what that says about the killers.

"What we tried to do was give investigators working these cases a common place to start, which is the body," Morton said. "You work your way back from there to discern offender characteristics and narrow the suspect pool. The body is the only constant in the crime," he explained. "Lots of other things can change, but how you find that victim is not going to change."

If the victim was a prostitute, for example, and the body was left where the murder occurred, that may offer certain clues about the killer. If the body was hidden at a distance from the murder site, that may offer different clues. The study's statistical data was drawn from 480 U.S. serial murder cases involving 92 offenders over a period of nearly five decades. Morton believes the study's findings could be a "game changer" for investigators working unsolved cases.

"Many of the things we have learned over the years through experience we are trying to prove through empirical research," he said. "The main goal is to provide

law enforcement with relevant data that helps them focus on the most likely suspects."

Serial murder in the United States is surprisingly rare. Although it's impossible to quantify the number of active serial murderers nationwide or how many murders they commit, academic and law enforcement research suggests that the numbers of homicides carried out by serial offenders in a given year are a fraction of the total number of murders that occur in the U.S. "But when it does occur," said Morton, who has worked dozens of these cases during his 25-year Bureau career, "it can be overwhelming to a community and its law enforcement agencies."

"There is a lot of pressure on the police to solve these crimes," he added, and most local police departments haven't had a serial homicide in their jurisdiction. That's where the FBI can provide behavioral-based investigative support to our state and local partners. The National Center for the Analysis of Violent Crime and members of our Behavioral Analysis Unit have extensive experience with serial murder investigations and offer their expertise on request.

"The FBI has become a clearinghouse for these crimes," Morton said, "and we stand ready to assist local law enforcement when they are faced with an active serial murder case. This new research is one more tool to help investigators."

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

Sex Trafficker Receives 40-Year Sentence

Texas Man Found Young Victims Through Social Media Sites

It is yet another example of how social media can be dangerous for young people. Recently, a Houston man was sentenced to 40 years in prison on child sex trafficking charges after identifying and contacting young girls through social media platforms and then luring them into prostitution.

Back in 2012, 20-year-old Tevon Harris—aka "Da Kidd" or "King Kidd"—didn't have a legitimate job. He lived on and off with his mother but mostly moved from one motel room to the next. And he was very good at manipulating people. Harris trolled social media websites looking for vulnerable young girls he could sexually exploit. Online, he complimented them. He offered them modeling jobs. And he promised them lots of money.

Some agreed to meet with him, and he would go and pick them up. But what waited for them was not the glamorous modeling world. It was a nightmarish world of motel rooms, forced sexual encounters—with Harris himself and then with paying customers—and other degrading and violent acts.

Harris used violence and intimidation to keep the girls cooperative. He took their wallets and their cell phones, cutting off their communication with the outside world. In one instance, he deprived a victim of food for four days because he thought she wasn't serving a client well enough. He also supplied her with marijuana and alcohol. Another victim was beaten with a towel rack torn from a motel room wall when Harris found her using a phone to call her mother for help. And he helped himself to all the money paid by customers.

Using photos he took or occasionally pilfered from the victims' own social media pages, Harris advertised the girls' services on various Internet websites.

The case was investigated by the FBI's Child Exploitation Task Force in Houston, one of many child-focused task forces that we participate in around the country, working side by side with our partner agencies to investigate individuals and criminal enterprises responsible for victimizing young people. The Houston task force works closely with the Houston Police Department—in particular, its Vice and Juvenile Sex Crimes Divisions—and it was Houston uniformed officers who recovered one of Harris' victims and subsequently notified the task force.

The task force collected enough evidence to convince Harris to plead guilty. There was also enough evidence to prompt the judge to order that—after serving his 40-year sentence—Harris spend the rest of his life on supervised release. He's also required to register as a sex offender.

The dangers and pitfalls of social media cannot be overstated, especially for young people. Here are a few tips on how to stay safe online:

- Only "friend" and connect to people online that you know personally.
- Set your social media security settings so that only confirmed friends and connections can see what you are posting.
- Never post a picture of yourself or write anything on social media sites—or in e-mails and text messages—that you wouldn't want the world to see.
- Be wary of giving anyone you meet through social media your phone number, e-mail address, or home address. Use common sense.
- And most importantly, be aware that anyone you meet online may not be who they say they are.

Color of Law

Agent Exposes Civil Rights Crimes in Alabama Prison

There was never any dispute that Rocrast Mack, a 24-year-old serving time on drug charges in a state prison in Alabama, died at the hands of corrections officers in 2010. What wasn't immediately clear was how and why the inmate sustained a lethal beating.

What was known was this: On August 4, 2010, a female corrections officer confronted Mack in his bunk, accused him of inappropriate behavior, and struck him. Mack retaliated, the officer radioed for help, more officers arrived, and Mack was beaten in three separate prison locations over a 40-minute period. He died the next day from his injuries. Guards claimed Mack fought them throughout the ordeal and sustained his fatal injuries in a fall.

An investigator from Alabama's State Bureau of Investigation thought the stories didn't add up and called the FBI, which investigates cases of abuse of authority—or color of law—and other civil rights violations. When Special Agent Susan Hanson opened her case at the Ventress Correctional Facility, her biggest challenge would be getting to the truth.

"The injuries that caused Mack's death did not match up with the story the corrections officers were telling," said Hanson, who works in the Dothan Resident Agency, a satellite office of the FBI's Mobile Division. Meanwhile, witness accounts were suspect, given the questionable reliability of the sources. "You could have 10 different inmates who were in the very same room and they would give you 10 different stories," she added.

What did emerge was a portrait of a corrupt prison environment led by a heavy-handed guard—Lt. Michael Smith. Smith, the main subject in the investigation, held sway over corrections officers and inmates alike. A few guards privately acknowledged that Smith's history of intimidation could eventually land him in hot water. For Hanson, who conducted hundreds of interviews over nearly three years, the key to cracking the case was to find a sympathetic guard whose conscience carried more weight than his fear of Smith.

"It really was working with one of the officers, spending a lot of time with him, and telling him that the story just doesn't make sense. It cannot have happened that way," Hanson said. The guard implicated Smith but never broke ranks from the original narrative—that their use of force was justified.

A view of the prison yard at the Ventress Correctional Facility in Alabama. The image was part of a display in court to show the perspectives of witnesses to the fatal 2010 assault of an inmate by corrections officers.

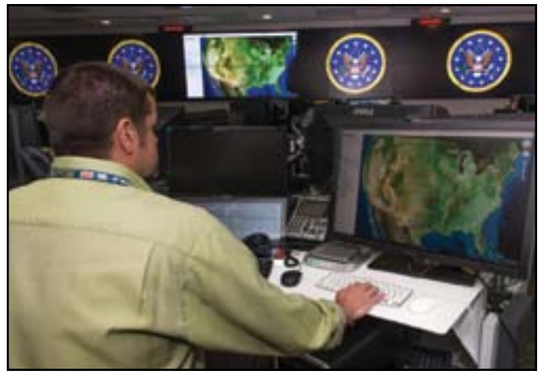
To build her case, Hanson and Special Agent William Beersdorf enlisted Mobile's Evidence Response Team (ERT) to take extensive photographs from witnesses' vantage points that could support or refute their claims. "That's where she was able to start separating fact from fiction," said Beersdorf. Specialists were brought in from the FBI's Charlotte office to collect exact measurements and chart graphical representations of where each of the assaults occurred.

"Susan then could eliminate witnesses because of what they could or couldn't see," said Bryan Myers, an ERT technician who made six trips to the prison during the course of the investigation. The Special Projects Unit at FBI Headquarters assembled an interactive blueprint of the prison that showed everyone's precise locations during the beatings. In the end, the evidence revealed how a cadre of guards, led by Smith, struck and kicked Mack so severely he died—and then conspired to cover it up.

"It was very helpful during trial," said Hanson. Four officers were convicted last year on civil rights, obstruction of justice, and conspiracy charges and received prison terms—including Smith, who was sentenced to 30 years.

Hanson, who was named a finalist for the Service to America Medal by the Partnership for Public Service for bringing the guards to justice and exposing corruption in Alabama's prisons, said the case is still heartbreaking to her because Mack was in the care of officials who had been bestowed a public trust.

"He was serving his time, he was not a problem child, and he was beaten to death because of conduct that had gotten out of control," she said.



Cyber Security

Task Force Takes 'Whole Government' Approach

Hackers compromising banking and retail networks to steal consumers' personal information. Foreign actors virtually accessing our trade secrets. Criminal groups lining their pockets by exploiting any online vulnerability they can find.

In today's virtual world, it is well known that cyber crime can jeopardize our privacy, our economy, and even our national security. Less well known is an organization—the National Cyber Investigative Joint Task Force (NCIJTF)—that is working around the clock to fight the threat.

"The challenge we face as a nation is formidable, because the bad actors never stop trying to infiltrate our systems," said Greg McAleer, an assistant special agent in charge at the U.S. Secret Service who was recently named one of the NCIJTF's deputy directors. "The NCIJTF uses a whole government approach—employing every tool in our arsenal to address the threat and protect our infrastructure, financial systems, and intellectual property."

Working largely out of public view, the nearly two dozen federal intelligence, military, and law enforcement agencies that comprise the NCIJTF—along with local law enforcement agencies and international and private industry partners—serve as the government's central hub for coordinating, integrating, and sharing information related to cyber threat investigations.

Established in 2008 by a presidential directive and administered by the FBI, the NCIJTF is also tasked with identifying cyber hackers and understanding their motivations and capabilities. That knowledge is used to disrupt criminal operations, minimize the consequences of intrusions, and ultimately bring perpetrators to justice.

Left: The National Cyber Investigative Joint Task Force serves as the government's central hub for coordinating, integrating, and sharing information related to cyber threat investigations.

This unified, government-wide approach leverages intelligence gathering and sharing among task force partners to gain a strategic view of what our enemies are trying to do within our infrastructure and why.

"Individual local and federal organizations rightfully focus on immediate threats in their areas of responsibility, but the NCIJTF is looking at the overall cyber landscape," said FBI Special Agent Paul Holdeman, an NCIJTF chief. "We are looking at the broad strategic shifts in the enemy's tactics and movements. What are these bad actors doing, and what threats do they pose?"

The ability to share intelligence across government agencies integrates the response to intrusions and investigations. "That is the key to the NCIJTF's success, the exchange of information," Holdeman said. "Bringing everyone together under one roof has been a huge benefit."

Gustavo Rodriguez, a lieutenant with the New York Police Department (NYPD), recently completed a six-month assignment on the task force as part of the FBI's Law Enforcement Fellows program, in which members of local law enforcement are trained so they can in turn train their colleagues when they return to their organizations.

"The NYPD has a robust cyber program," Rodriguez said, "but the department thought it would be wise to see how the NCIJTF collectively addresses the cyber threat. The Fellows program allowed me to see the threat in real time domestically and internationally." He added, "This experience has opened my eyes to how serious the threat is and how much damage bad actors could cause if left unchecked."

The cyber criminals and nation states probing our systems are relentless, McAleer said. "But the American public should know that the NCIJTF will leverage technology, intelligence, tactics, and partnerships to disrupt attacks before they materialize."

Agencies Cooperate in Child Sexual Exploitation Case

Michigan Subject Gets 30 Years in Prison

According to the federal judge who heard the case, the defendant's conduct was "about as serious as it gets," and that on a scale of one to 10, she believed the case was "way past 10." Then she sentenced the defendant—James Alfred Beckman, Jr. of Grand Rapids, Michigan—to 30 years in prison.

What crimes moved the judge in this case to hand down such a substantial prison term? Multiple counts of attempted sexual exploitation of a child, attempted coercion of a child, and receipt and distribution of child pornography. And in addition to the lengthy prison stay, the judge also imposed a lifetime term of supervised release on the defendant once he gets out, ordering that he register as a sex offender.

The success of this case, as with many investigations involving the FBI, can be attributed to the close working relationship between Bureau investigators and our partners—in this instance, troopers from the Michigan State Police (MSP) and prosecutors from the U.S. Attorney's Office for the Western District of Michigan. The agencies' seamless interactions resulted in the incarceration of an individual who posed a very dangerous threat to children.

The investigation into the illicit activities of Beckman began in September 2012, when a woman came to the MSP with allegations that Beckman had sexually abused her young child. The youngster reported that during the abuse, a computer and webcam had been present. Troopers opened a case and involved the state's Child Protective Services to conduct interviews of the young victim and another child by an expert who is specially trained to interact with children who are victims of crime.

MSP investigators interviewed Beckman and performed forensic exams on his computers. The examination of Beckman's work laptop turned up not only photos of child pornography but also evidence of a network of individuals trafficking in child pornography. It was at that point—when the MSP determined that Beckman's activities had

spread outside the state of Michigan—that FBI assistance was solicited, and we opened a case in October 2012.

Continuing to work together, the MSP and FBI obtained evidence of online chats that Beckman had with others in his child pornography network. During many of the chats, Beckman was soliciting individuals who were conducting sexual acts with children, usually encouraging conversations about these activities and exchanging pornographic images and videos with them. Working to identify those in the network, the Bureau sent out leads to a number of our field offices around the country and several of our legal attaché offices overseas.

A unique set of circumstances surrounded the sexual exploitation charges. Evidence presented at trial showed that Beckman sexually abused and exploited two young children, and he streamed and attempted to stream live video of this abuse and exploitation to others. Because he streamed his child pornography via webcam, we had no images or videos to enter as evidence. However, we managed to track down a number of people Beckman streamed to—and two of them testified against him in court. One of those two individuals was charged, pled guilty, and was sentenced to a 12-year prison term. Charges are pending against the second.

After a two-week trial during which one of the young victims testified against Beckman from a room outside the courtroom, a jury found the defendant guilty on 15 of the 16 charges against him.

Left: Nigerian criminals behind purchase order frauds use fake or stolen e-mail addresses to deceive retailers, as shown in the example at left. They also dupe individuals who are the victims of online romance or work from home scams to re-ship merchandise out of the country, as seen in the example at right.

Cyber Crime

Purchase Order Scam Leaves a Trail of Victims

What began as a scheme to defraud office supply stores has evolved into more ambitious crimes that have cost U.S. retailers millions of dollars—and the Nigerian cyber criminals behind the fraud have also turned at-home Internet users into unsuspecting accomplices.

FBI investigators are calling it purchase order fraud. Through online and telephone social engineering techniques, the fraudsters trick retailers into believing they are from legitimate businesses and academic institutions and want to order merchandise. The retailers believe they are filling requests for established customers, but the goods end up being shipped elsewhere—often to the unsuspecting at-home Internet users, who are then duped into re-shipping the merchandise to Nigeria.

"They order large quantities of items such as laptops and hard drives," said Special Agent Joanne Altenburg, who has been investigating the cyber criminals since 2012 out of our Washington Field Office. "They have also ordered expensive and very specialized equipment, such as centrifuges and other medical and pharmaceutical items."

Our investigators have found more than 85 companies and universities nationwide whose identities were used to perpetrate the scheme. Approximately 400 actual or attempted incidents have targeted some 250 vendors, and nearly $5 million has been lost so far.

The scam has several variations, but basically it works like this:

- The criminals set up fake websites with domain names almost identical to those of real businesses or universities. They do the same for e-mail accounts and also use telephone spoofing techniques to make calls appear to be from the right area codes.
- Next, the fraudsters—posing as school or business officials—contact a retailer's customer service center and use social engineering tactics to gather information about the organization's purchasing account.
- The criminals then contact the target business and request a quote for products. They use forged documents, complete with letterhead and sometimes even the name of the organization's actual product manager. They request that the shipments be made on a 30-day credit—and since the real institution often has good credit, vendors usually agree.
- The criminals provide a U.S. shipping address that might be a warehouse, self-storage facility, or the residence of a victim of an online romance or work-from-home scam. Those at-home victims are directed to re-ship the merchandise to Nigeria and are provided with shipping labels to make the job easy.
- The vendor eventually bills the real institution and discovers the fraud. By then, the items have been re-shipped overseas, and the retailer must absorb the financial loss.

Although the cyber criminals are practiced at deception, there are ways to spot the fraud, according to Special Agent Paula Ebersole in our Washington Field Office. "The most important thing is to independently verify shipping addresses," she said, "no matter how legitimate a website or e-mail looks."

Businesses should also be on the lookout for e-mails that contain unusual phrases or spellings, indicating that messages were not written by a fluent English speaker. And bogus phone numbers provided by the fraudsters are rarely answered by a live person.

"If your business has been scammed," Ebersole added, "time is of the essence. If you report the theft to local authorities or the FBI before the merchandise is shipped out of the country, there is a chance the items can be located and returned."

In addition to investigating these crimes, Ebersole and Altenburg are also getting the word out to the business community about purchase order fraud through the Domestic Security Alliance Council, a security and intelligence-sharing initiative between the FBI, the Department of Homeland Security, and the private sector. "We want to make everyone aware of this potential threat."

Ten Years of Protecting Children

International Task Force Targets Pedophiles, Rescues Victims

Ten years ago this month, the FBI stood up the Innocent Images International Task Force. Its mission: to investigate commercial websites—at that time mostly based in Eastern Europe—involved in the worldwide distribution of child pornography. A big task for a small but dedicated group of expert investigators from the U.S. and five other participating nations.

Fast forward to October 2014, and this group of investigators has grown from about a half dozen individuals to around 60 officers from nearly 40 countries. And the group's changed name—the Violent Crimes Against Children International Task Force—represents its expanded mission today: to identify and bring to justice anyone involved in violent child sexual exploitation activities, whether online or in person, and to identify and rescue the victims of these crimes no matter where in the world they may be.

The FBI created the task force to help counteract some of the difficulties that we—and other law enforcement agencies around the world—were facing while investigating complex, multinational child sexual exploitation cases. Constantly changing technology helped pedophiles prey on children anywhere and made law enforcement detection difficult. And law enforcement had to work within the context of political, legal, and judicial cooperation mechanisms that predated the digital era.

So how does the task force maneuver through these difficulties?

- For one, to help standardize investigations and enhance capabilities, the Bureau provides the same training to all task force officers in areas like online investigations, interviewing and interrogation, behavioral analysis, victim assistance, FBI priorities, and U.S. judicial standards.
- Also, putting task force officers together in the same room for training—and for a yearly case coordination meeting—helps establish professional relationships that carry over into the investigative arena, facilitating the real-time sharing of intelligence and the working of joint operations.

- And lastly, by combining forces, resources, and expertise, law enforcement collectively becomes more effective in identifying and taking down these criminal networks around the world.

Today, as we did 10 years ago, the FBI—with the help of our legal attaché offices overseas—seeks the best and the brightest to join the task force. Working alongside Bureau agents who specialize in these kinds of cases are task force officers with similar experience in their own countries, who come mainly from national-level police agencies, who have an understanding of cyber technology, and who are deeply committed to working with their international colleagues to protect children everywhere from sexual exploitation.

Obviously, our goal is to identify and prosecute these sexual predators, but we also want to identify and rescue their vulnerable victims. One of the ways we do that is through Operation Rescue Me, a joint FBI/National Center for Missing & Exploited Children program that uses image analysis to determine the identity of victims depicted in child sexual exploitation material.

Over the years, the Violent Crimes Against Children International Task Force has played a key role in a number of international cases. And looking ahead, we will continue to effectively target and take down those who threaten the youngest and most vulnerable among us by continually adapting our law enforcement response to the ever-changing nature of the threat.

Virtual Kidnapping

U.S. Citizens Threatened by Mexican Extortion Scheme

Jose Ramirez, a retired New York police officer and ultra-fit triathlete, is an unlikely victim. But last December in Cancun, Mexico, after completing an Ironman competition, he was tricked into believing his life was in danger. Like an increasing number of U.S. citizens on both sides of the border, Ramirez was the target of an extortion scheme known as virtual kidnapping.

Unlike traditional abductions, virtual kidnappers do not intend to physically detain their victims. Instead, through various deceptions and threats of violence, they coerce individuals to isolate themselves from their families—or make families believe that their loved ones are being held—all to extract a quick ransom before the scheme falls apart.

"Victims of virtual kidnappings are scared for their lives, and so are their families," said Special Agent Brian Wittenberg, a member of our International Violent Crimes Unit at FBI Headquarters who has worked many of these cases.

Although these extortion schemes have been around for many years, their numbers are on the rise, and the criminals' tactics are becoming more sophisticated. "It's big business for them, and they do it well," Wittenberg said. "Since the threat is continuing to evolve, the FBI wants to raise public awareness to help individuals from becoming victims."

After completing the rigorous Ironman—a 2.4-mile swim, 112-mile bike ride, and marathon run—the 73-year-old Ramirez returned to his hotel room in the evening, called his wife at home in Nevada, and went to sleep. Around 1 a.m., the phone rang in his room. A man claiming to be a member of the Zetas, a ruthless drug cartel, said Ramirez was being "fined" $10,000.

They knew his name and information about him, possibly from accomplices at the hotel. "They were very believable, and they were making threats," Ramirez said, recalling the threats: "If you don't listen to us, we are going to put drugs in your hotel room and you're going to rot in jail in Mexico. Or we will just put a pistol to your head and kill you."

What followed for Ramirez was a nearly three-day ordeal in which he was instructed to change hotels, buy a new cell phone—so his wife could not reach him—and withdraw money from the bank. "And don't forget, we are watching you," he was told. Eventually, his wife contacted local law enforcement who, in turn, called the FBI. With the help of Mexican police, Ramirez was recovered unharmed.

Although millions of Americans safely visit Mexico each year for business and pleasure, they can be targets for virtual kidnappers. "People with family and connections in Mexico and communities on both sides of the border have legitimate fears of the gangs and drug cartels and how violent they are," said a member of our Crisis Negotiation Unit who has worked many hostage situations. "That fear plays into the hands of the virtual kidnappers," he said. "They use it to their advantage."

"If you think you are a victim, get to a place that feels safe, and then call someone who can help," said the crisis negotiator. "If you are a family member or loved one getting ransom calls, remember that you have more power than you think, because you have the money that the kidnappers want." He added that while some families think they can handle these situations alone, the FBI—which is the lead investigative agency when a U.S. citizen is taken hostage overseas—stands ready to offer its expertise and guidance to frightened families. "We can help," he said.

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

Egregious Case of Health Care Fraud

Cancer Doctor Admits Prescribing Unnecessary Chemotherapy

Imagine receiving a diagnosis of cancer and then having to go through chemotherapy or other intensive treatments. Then imagine finding out that you never had cancer in the first place and that your doctor—whom you trusted implicitly—merely used you in his scheme to fraudulently bill the federal Medicare program and private insurance companies for hundreds of millions of dollars.

That's exactly what happened to patients of Dr. Farid Fata, a Detroit-area hematologist and oncologist. And it was not only cancer diagnoses. Some patients were told, wrongly, that they had other conditions which required expensive intravenous therapies, medications, and diagnostic tests—all of which jeopardized their health and well-being.

But after a thorough investigation by the FBI, Department of Health and Human Services' Office of Inspector General (HHS-OIG), and the Internal Revenue Service-Criminal Investigations (IRS-CI)—and just before his trial was scheduled to begin—Fata recently pled guilty to 13 health care fraud crimes against his patients, as well as one count of conspiracy to receive kickbacks and two counts of money laundering.

Fata operated a cancer treatment clinic—Michigan Hematology Oncology, P.C.—which had multiple locations throughout Michigan. He also owned a diagnostic testing facility—United Diagnostics, PLLC—in Rochester Hills, Michigan. His case came to light in the summer of 2013, when allegations against him came to the attention of the U.S. Attorney's Office for the Eastern District of Michigan and the Medicare Fraud Strike Force from the Department of Justice's (DOJ) Criminal Division.

Because of the seriousness of the allegations and the potential risk to the health of Fata's current patients and any future patients, FBI and HHS-OIG investigators, as well as Assistant U.S. Attorneys and DOJ Criminal Division prosecutors, moved quickly to collect corroborating information from employees in his practice. Within days, there was enough evidence to arrest him and shut down his businesses.

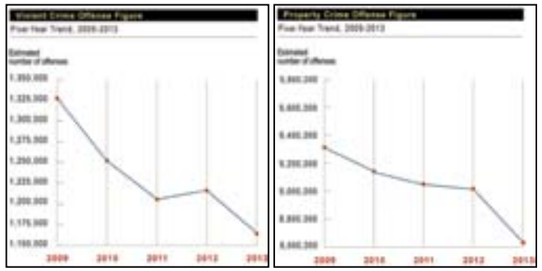
After his arrest, agents, prosecutors, and staff at each of the involved agencies worked around the clock to ensure that all of Fata's patients—past and present—got their medical files so they could receive continued care. Investigators and prosecutors also contacted major medical centers in the southeastern Michigan area to ensure that Fata's patients would be taken in quickly by new treating physicians.

In the months that followed, agents and prosecutors pored over billing data, medical records, financial records, and other materials recovered in searches of Fata's businesses. In addition, agents interviewed hundreds of witnesses, including employees, former patients, and family members of patients.

Fata's plea to the health care fraud charges, kickback conspiracy, and money laundering was the culmination of an intensive and extensive investigation. Some of the conduct he admitted to in his guilty plea included:

- Administering unnecessary chemotherapy infusions;
- Administering unnecessary iron infusions;
- Administering unnecessary human growth factors;
- Ordering unnecessary cancer tests;
- Accepting kickbacks to refer patients for home health care services; and
- Promoting his cancer test fraud scheme with money laundered from his infusion fraud scheme.

At his upcoming sentencing, Fata faces up to 175 years in prison on the charges he pled guilty to. The U.S. Attorney has stated that prosecutors intend to seek life.



Left: Charts from the just-released *Crime in the United States, 2013* publication show the downward progression in the number of reported violent crimes (left) and property crimes (right) over the past five years.

Crime Statistics for 2013 Released

Decrease in Violent Crimes and Property Crimes

The FBI released *Crime in the United States, 2013* today, which shows that the estimated number of violent crimes in 2013 decreased 4.4 percent when compared with 2012 figures, and the estimated number of property crimes decreased 4.1 percent. There were an estimated 1,163,146 violent crimes reported to law enforcement last year, along with an estimated 8,632,512 property crimes.

The crime statistics report, issued by the Bureau's Uniform Crime Reporting (UCR) Program, contains voluntarily submitted data from 18,415 city, county, state, tribal, campus, and federal law enforcement agencies on specific crimes brought to their attention. They include the violent crimes of murder, rape, robbery, and aggravated assault, and the property crimes of burglary, larceny-theft, motor vehicle theft, and arson.

The primary goals of *Crime in the United States*? To assess and monitor the nature and type of crime in the nation and to generate reliable information for use in law enforcement administration, operations, and management. The data has also been used by criminologists, sociologists, legislators, municipal planners, the media, and other students of criminal justice for research and planning purposes.

But a word of caution: Don't draw conclusions from the report by making direct comparisons between cities. Valid assessments are only possible with an understanding of various factors affecting each jurisdiction.

Beginning in 2013, the UCR Program began collecting rape data under a revised definition. However, not all law enforcement agencies have been able to convert their records management systems to reflect the new definition yet, so this year's report includes data collected under the previous (or legacy) definition as well as the revised definition. Footnotes for tables in the report indicate which definition of rape is being used.

Here are some quick highlights from *Crime in the United States, 2013:*

- During 2013, law enforcement made an estimated 11,302,102 arrests (including 480,360 for violent crimes and 1,559,284 for property crimes). The highest number of arrests were for drug abuse violations (estimated at 1,501,043), larceny-theft (estimated at 1,231,580), and driving under the influence (estimated at 1,166,824).
- There were an estimated 14,196 murders last year.
- Aggravated assaults (an estimated 724,149 last year) accounted for the largest percentage of violent crimes reported to law enforcement—62.3 percent.
- Firearms were used in 69 percent of the nation's murders, 40 percent of robberies, and 21.6 percent of aggravated assaults (weapons data is not collected on rape incidents).
- There were an estimated 79,770 rapes (legacy definition) reported to law enforcement.
- Victims of burglary offenses suffered an estimated $4.5 billion in property losses, and burglaries of residential properties accounted for 74 percent of the total reported.
- Larceny-thefts accounted for the largest percentage of property crimes reported to law enforcement—69.6 percent. (The average value of property taken during larceny-thefts was $1,259.)
- During 2013, an estimated 699,594 motor vehicles were reported stolen, and 73.9 percent of those were cars. (Other types of stolen vehicles included trucks, sport utility vehicles, buses, motorcycles, motor scooters, all-terrain vehicles, and snowmobiles).

UCR publications scheduled for release within the next couple of months include *Law Enforcement Officers Killed and Assaulted, 2013*; *Hate Crimes Statistics, 2013*; and *National Incident-Based Reporting System, 2013*.

Child Pornography Case Results in Lengthy Prison Sentences

Couple Abused Child in Their Care

It was a horrific instance of child sexual exploitation that went on for approximately three years. But in the end, Patricia and Matthew Ayers—who pled guilty to crimes against a child in their custody—were recently sentenced to an astonishing 2,340 years collectively behind bars (1,590 for her, 750 for him).

The federal judge who handed down those sentences told the defendants, "I have been on the bench since 1998 and this is the worst case I have personally dealt with .... You robbed this child of her childhood and her soul, and a maximum sentence is the only sentence appropriate."

The case began in Alabama in December 2012, when a friend of the couple contacted local authorities after seeing digital pornographic pictures of a child that were provided to him by Patricia Ayers. The Lauderdale County Sheriff's Office served a search warrant at the Ayers' residence in Florence and seized computers, cell phone, cameras, and electronic storage media devices. Patricia Ayers—who admitted taking the images of the child, initially claiming they were taken for the purposes of documenting a rash—was arrested.

Found among the thousands of pornographic images on the seized devices were pictures of Matthew Ayers and the young victim engaged in sexual acts—he was then arrested by local authorities as well.

In early January 2013, Lauderdale authorities requested the Bureau's assistance, and our Florence Resident Agency (out of the FBI Birmingham Field Office) opened a federal child pornography investigation.

Another search warrant was served at the Ayers' residence to locate and document items seen in the child pornography images suspected of being produced in the home. A previous address that the pair had occupied was also searched—with the consent of the current homeowners—and law enforcement identified wallpaper in that house as the same wallpaper visible in some of the images.

During the course of the investigation, an agent from our Dallas Field Office who was working another child pornography matter was able to connect his case—and his subject—to Patricia Ayers through an automated search of FBI records. Among other links, Patricia Ayers had e-mailed the subject of the Dallas case images of child pornography, including pictures of the child in the Ayers' custody. Matthew and Patricia Ayers were indicted on federal charges in May 2014.

Assisting Bureau agents on the Ayers case was an FBI Computer Analysis and Response Team expert who reviewed all of the digital evidence seized during the search warrants, as well as FBI analysts who carefully scrutinized every image for clues as to when and where it was taken, what was being shown, and who was pictured.

Also involved were forensic child interviewers from our Office for Victim Assistance at FBI Headquarters, who are specially trained to get young crime victims and witnesses to talk about what they experienced while not traumatizing them any further. And FBI Birmingham's local victim specialist worked with the victim from the beginning of the case through sentencing and beyond, offering much-needed support, some counseling, and additional community resource referrals. The victim—who is believed to have been around 6 years old when the abuse started—is now in the care of family members.

This case and others like it demonstrate the value of—and the need for—law enforcement's lawful access to digital media.

Prison Plot Foiled

Murder Witness Threatened from Jail

It's one of the more outrageous prison plots the FBI has investigated in recent memory: An Ohio inmate—and the clinical psychologist who was in love with him—were among five people indicted last month and charged with threatening a murder witness.

"I've seen a lot of creative inmates trying to get released," said Special Agent Eric Rardain, who investigated the case out of our Philadelphia Field Office, "but never in my 22 years of law enforcement have I seen anyone go to this extreme."

Nicholas Stanishia, who is serving a life sentence at the Southeastern Correctional Institution in Lancaster, Ohio, apparently believed he could get out of jail if the man who saw him kill his ex-girlfriend recanted his testimony.

In 1997, Stanishia murdered his former girlfriend and shot her then boyfriend, who survived and later testified to what he saw. Stanishia was on the run for three years, during which time he also committed a home invasion and rape. At his murder trial in 2001, based on the witness' testimony, Stanishia was found guilty and received a life sentence.

To carry out his witness threat plan, Stanishia needed an ally on the outside—and he had one in Marcia Weber. The two had met years earlier when Weber was starting her clinical psychology career at a local prison where Stanishia was incarcerated on unrelated charges. Theirs was initially a doctor-patient relationship, but around 2006, after years of keeping in touch, Weber professed her love for him and began to help him orchestrate the scheme they hoped would win his freedom.

"It was apparent in the investigation that Dr. Weber was head over heels for Stanishia. She even sent him nude pictures of herself," Rardain said, explaining that the two exchanged hundreds of calls, and although she did not work at the institution where Stanishia was an inmate, she visited him monthly and wrote often, signing some letters, "Your loving wife."

Stanishia and Weber allegedly hired a private investigator to find out where the murder witness and his wife lived and worked as well as information about their children. Then they allegedly hired a man to place a gas can on the porch at the witness' family home in Pennsylvania.

According to the indictment, a fellow inmate helped smuggle a cell phone into the prison, which Stanishia used to call the witness and ask if he had received his previous "message." Stanishia claimed to be a ranking member of the Aryan Brotherhood and suggested that the witness sign a new affidavit—being prepared with Weber's help—recanting his original testimony. He told the man the Aryan Brotherhood could easily reach him and his family. "I want you to think about this," Stanishia said.

The frightened witness called local law enforcement, who contacted the FBI. It didn't take long for investigators to unravel the scheme.

"This was a well-calculated threat," Rardain said, "but the witness did the right thing by contacting law enforcement." He added that while "Stanishia is the bad guy here, he could not have carried out the threat without Weber. We believe she was coordinating the entire plan."

In October, Stanishia and Weber, along with three other accomplices—two of whom are already in jail—were indicted and charged with three counts relating to an interstate conspiracy to transmit threats to a witness. Weber is being held without bond. Trial is scheduled for December 3, 2014.

Honoring the Fallen

20 Years Since Shooting Killed Two Agents, Police Sergeant

Two decades ago, on November 22, 1994, a lone gunman entered the headquarters building of the Metropolitan Police Department (MPD) in Washington, D.C. and opened fire in a squad room, killing a police sergeant and two FBI agents. For those close to the fallen, who gathered today for a memorial service marking 20 years since the tragic event, it's as if it happened yesterday.

"Twenty years have passed, but our hearts are still heavy," said former FBI Director Louis J. Freeh, who headed the Bureau in 1994. "Our hearts and memories still feel the pain of that day. It was a day that we will never forget and will always honor."

Special Agents Michael J. Miller and Martha Dixon-Martinez, of the FBI's Washington Field Office, and MPD Sgt. Joseph "Hank" Daly were fatally wounded in the attack. Another FBI agent, John Kuchta, was seriously wounded, and a 15-year-old bystander was injured. The assailant, Benny Lee Lawson, was killed in the exchange of gunfire. The 25-year-old had been questioned as a suspect a week earlier in a triple homicide investigation

Nearly 500 guests attended the memorial service this morning at St. Patrick's Church in Washington, D.C., where FBI Director James Comey, Attorney General Eric Holder, and MPD Chief of Police Cathy L. Lanier joined family members and former colleagues of the service martyrs to reflect on their lives and contributions. Family members who spoke at the memorial asked that their fallen siblings be celebrated for how they lived.

Paul Dixon recalled a story about his sister, Martha, who threatened to quit her elementary school when it wanted to move her into a higher-level class. She didn't want to leave her friends. Dixon said the same was true when her fellow squad members were attacked 20 years ago. She could have escaped, but stayed to help her colleagues.

"She was going to stay there and fight for her friends and defend them. And that's what she did. That's an illustration of Martha's character. That's the woman that was taken from us," Dixon said. "So I would encourage everybody here not to focus on the deaths of these people. It's not how they died that made them heroes, but it's how they lived."

Many recalled how dangerous the city was in 1994 and credited the work of the Cold Case Squad—created in 1991 to solve moldering homicide cases—with helping turn the city around.

FBI Director James Comey speaks at a memorial service recognizing the 20-year anniversary of the fatal attack on two FBI agents and a Metropolitan Police Department sergeant at police headquarters.

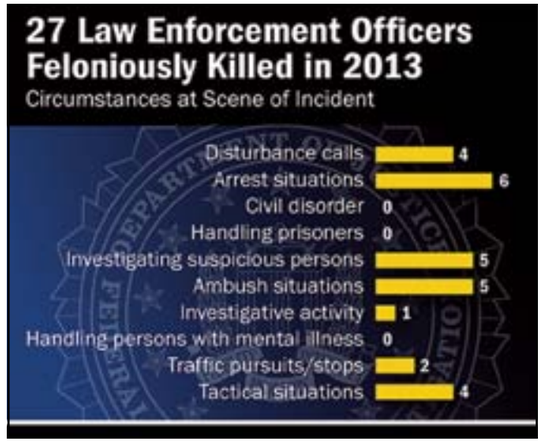
"It's incumbent upon us to remember that whatever we accomplish, whatever we achieve, we achieve standing on their shoulders," said Mike Daly, brother of Sgt. Hank Daly.

"When the moment came, when danger threatened, they ultimately gave what President Abraham Lincoln once called that last full measure of devotion to their families, to their colleagues, and to their country," said Attorney General Holder.

The two-hour service was followed by a procession to the National Law Enforcement Officers Memorial, where family members laid wreaths next to the names of their loves ones etched in the marble walls.

"Let's not dwell long on the anguish of that day," said Tony Daniels, who was in charge of the Washington Field Office in 1994. "Let's celebrate how they lived and how we can be proud of what they accomplished. Let's leave here today rededicating ourselves to what they taught us and what they represent: honor, courage, commitment."

Michael J. Miller | Sgt. Joseph "Hank" Daly | Martha Dixon-Martinez



In the Line of Duty

Law Enforcement Officers Killed and Assaulted, 2013 Report Released

A Florida sheriff's officer, responding to a report of a domestic disturbance at a residence, was shot and killed by someone inside the home. An Iowa police officer was shot and killed while attempting to serve an arrest warrant. A Michigan state trooper was fatally shot during a routine traffic stop. And a West Virginia sheriff was ambushed and fatally shot in the head while he was eating his lunch in a marked car.

According to the just-released *Law Enforcement Officers Killed and Assaulted* (LEOKA) report, these four officers were among the 76 men and women killed in the line of duty during 2013—27 died as a result of felonious acts, and 49 died in accidents. Another 49,851 law enforcement officers were victims of line-of-duty assaults. Proof positive of the dangers that all officers willingly face, day in and day out, to protect the rest of us.

Among the report's findings for 2013:

- Of the 27 officers feloniously killed, 16 were on assigned vehicle patrol duty when the incidents occurred, and all but one of the 27 officers was killed with a firearm.
- Circumstances surrounding the deaths of these 27 officers included arrest situations, ambushes, investigations of suspicious persons, disturbance calls, tactical situations, traffic pursuits or stops, and investigative activities.
- Law enforcement agencies identified 28 alleged assailants in connection with the felonious line-of-duty deaths (20 had prior criminal records).
- Of the 49 officers accidentally killed, 23 died as a result of automobile accidents.
- Of the nearly 49,851 officers assaulted during 2013, the largest percentage of victim officers (31.2 percent) were responding to disturbance calls (family quarrels, bar fights, etc.) when the incidents occurred.

New to LEOKA is the addition of detailed data concerning assault victims. Although this year's detailed information on assaults was only received for 78 officers, submissions are expected to increase over time.

The LEOKA publication, released by the FBI's Uniform Crime Reporting (UCR) Program, contains data on duly-sworn city, university/college, county, state, tribal, and federal law enforcement officers who, at the time of the incidents, met the following criteria:

- They were working in an official capacity, whether on or off duty;
- They had full arrest powers;
- They ordinarily wore/carried a badge and a firearm; and
- They were paid from government funds set aside specifically for sworn law enforcement representatives.

The information in the report comes from various sources—the law enforcement agencies participating in the UCR Program, FBI field offices, and several non-profit organizations, such as the Concerns of Police Survivors and the National Law Enforcement Officers Memorial Fund.

The goal of the FBI's LEOKA program is to provide data and training that help keep law enforcement officers safe as they serve and protect our nation's communities. Later this week on our website, we'll focus on what LEOKA is doing, beyond its annual report, to further that goal—specifically, the extensive research being done on collected data (including studies involving interviews with individuals convicted of police killings) and the incorporation of that research into the officer safety awareness training conducted by the LEOKA program for partner agencies.

In the Line of Duty

Annual 'Officers Killed' Report More Than a Tally of Losses

The FBI's annual *Law Enforcement Officers Killed and Assaulted* (LEOKA) report released earlier this week details in chilling narratives and statistics how 76 law enforcement officers were killed in the line of duty in 2013.

While the LEOKA report offers a stark reminder of the dangers police face every day, the main reason for gathering the comprehensive data about line-of-duty fatalities, assaults, and accidents is to prevent them from occurring in the future. In addition to collecting details about the critical aspects of fatal confrontations and assaults, the FBI's LEOKA program conducts extensive research on the data that eventually gets incorporated into the officer safety awareness training the FBI provides for partner agencies.

"It's a three-prong program," said Brian McAllister, a training instructor for LEOKA, a unit in the Bureau's Criminal Justice Information Services (CJIS) Division. "LEOKA is about data, it's about research, and it's about training."

The data is collected from participating agencies across the country as part of the Uniform Crime Reporting Program and is published in conjunction with *Crime in the United States*, the FBI's annual dissemination of crime statistics. Over the years, researchers led by the LEOKA program have performed deep-dives into the data and published research aimed at giving officers a sharper understanding of what types of scenarios and circumstances have resulted in fatalities and assaults—and how to avoid them. The research delves well beyond statistics to include in-depth interviews with officers who were victims of assaults or involved in incidents that resulted in officer fatalities. The LEOKA program staff—former police officers—also interview the perpetrators of police deaths, hoping to provide a window into what compelled them to make a fatal move on a law enforcement officer.

For officers going through LEOKA's Officer Safety Awareness Training, it's these first-hand accounts that bring the job's dangers to the fore. "It's a wake-up call for officers in the class to see and listen to an interview with an offender who has killed a police officer," said McAllister, who conducts some of the interviews in addition to teaching the eight-hour seminars.

"It makes a huge impact on these guys," said Lt. Herb Rosenbaum, of the Trussville Police Department near Birmingham, Alabama. "When we're out on the road, we all have a tendency to fall into a routine. You've made a thousand traffic stops and you've never been challenged. This brings it back to the forefront."

The LEOKA program has released three multi-year studies tailored toward improving officer safety—*Killed in the Line of Duty* (1992), *In the Line of Fire* (1997), and *Violent Encounters* (2006). Each zeroed in on a subset of fatality and assault cases in prior years and looked for common threads that might illustrate better ways to assess or respond to a situation.

More recent statistics have shown a significant uptick in ambushes and unprovoked attacks on police, which prompted the LEOKA program to embark on a new study in 2013 that will include the unique perspectives of ambush victims and perpetrators. The study, due out in 2016, is reviewing cases from 1995 to 2011, looking for general themes of offender motives and officer perceptions.

"We want to figure out why the offenders were doing what they were doing and how the police officers reacted to see if there's anything we can link in the study that would enhance police officer safety," said James Sheets, a LEOKA training instructor.

Special Agent Michael Freeman, who coordinates training for our Norfolk Field Office, said LEOKA training is popular with police departments and other agencies in his region. He said the sobering information and first-person accounts help ensure against complacency.

"What adds so much value," Freeman said, "is receiving the perception of the offender and why that individual made the decision to challenge that law enforcement professional."

Left: Chemical storage tanks provided a visual aid during an FBI-led exercise in Houston designed to test emergency responders in the event of a chemical attack.

WMD Training

FBI Worst-Case Exercise Tests Response to Chemical Attack

When the facility manager for a hazardous waste disposal company near Houston took his seat at the table with law enforcement officials and emergency first responders, he knew it was going to be a very bad day. In the coming hours, his facility would experience a break-in, a fire, and the theft of a chemical agent that would be intentionally released at a popular waterfront amusement park, sending a poisonous plume across the region.

The fictional worst-case scenario was designed by the FBI's Chemical Countermeasures Unit—part of our Weapons of Mass Destruction (WMD) Directorate—to shake out any weaknesses in the region's elaborate network of emergency responders. The daylong exercise, attended by more than two dozen local, state, and federal agencies, raised all the tangly issues that come up in real catastrophic events: Who has jurisdiction? Who is the lead investigative agency? Who is qualified to appropriately respond?

"It's an excellent opportunity for everybody to get together and learn what each other's capabilities are," said Special Agent Amanda Koldjeski, a WMD coordinator in the FBI's Houston Division, which hosted the training event in October as part of the Bureau's ongoing effort to reach out to first responders and high-risk chemical facility operators about potential threats in their areas.

The exercise also showed how private industry has an important seat at the table in dynamic events like this, since they know their materials and vulnerabilities better than anyone else, and they are most likely to be the first to recognize suspicious activity related to their own operations.

"As a manager you never want to be responsible for something like this going on," said Bruce Shelton, manager of the waste disposal site in La Porte, just outside of Houston, that was targeted in the exercise (the Houston area is home to the largest concentration of chemical facilities in the U.S.). "But I know that we absolutely need to be in contact with our local emergency planning folks in this type of environment, because we don't know what's going to happen tomorrow."

In the scenario, things go from bad to worse very quickly, and agency representatives are confronted with real-time questions about how they will respond in what is emerging as an act of domestic terrorism. Who is the incident commander? Is this an ongoing attack? Are we evacuating? Are your people trained to operate in personal protective equipment? Do they have access to that equipment? Knowing the roles and skills of all parties in advance can reduce confusion in a real incident, whether it's a terrorist attack or an accident.

"We have a lot of incidents that happen in this part of the country, so I think it's good for us to review those so we hopefully limit the number of potential mistakes," said Mark Sloan, coordinator of the Harris County Office of Homeland Security and Emergency Management. "Any time you get face time with your partners, it's going to benefit you when you meet at 2 a.m. and say, 'Hi, what resources do we have available to us?'"

Each of the FBI's 56 field offices has at least one WMD coordinator whose job includes establishing relationships with local partner agencies and private companies to prevent WMD attacks. In making the rounds, the coordinators share prevailing threats and become key points of contact when a suspicious incident arises in the WMD arena.

"Our WMD coordinators are the face of the Bureau when they go out and meet the locals," said Chris Freeze, assistant special agent in charge of the Houston Division, who participated in the exercise.

Bruce Shelton, the facility manager, had never dealt with most of the individuals or agencies that participated in the exercise. Seeing the response unfold in front of him gave him a fresh perspective on his own role in securing his site and helping in a coordinated response.

"There are a lot of resources out there that I haven't used until now," he said after the scenario concluded. "It's good to know where they're at and who they are."

New Top Ten Fugitive

Help Us Find a Murderer

Yaser Abdel Said, wanted for the murder of his two teenage daughters in Texas, has been named to the Ten Most Wanted Fugitives list. A reward of up to $100,000 is being offered for information leading directly to the arrest of Said, who was born in Egypt and may be hiding there or in U.S. communities with Egyptian ties.

On January 1, 2008, Said persuaded his estranged daughters—Amina, 18, and Sarah, 17—to visit him. He said he was going to take them to get something to eat. Instead, he allegedly drove them in his taxi cab to a remote location and used a handgun to murder them. One of the girls was able to make a 911 call and was heard screaming for help, saying she and her sister were being shot by their father. Their bodies were discovered several hours later in the cab, which was abandoned outside a hotel in Irving, Texas.

"Yaser Abdel Said is wanted for his alleged role in committing a terrible act of violence against his own daughters," said Diego Rodriguez, special agent in charge of our Dallas Field Office. "Adding him to the Ten Most Wanted Fugitives list shows our commitment to seek justice for Amina and Sarah."

Since the murders nearly seven years ago, the case has received widespread publicity, and law enforcement has followed every credible lead, but Said remains at large. Today's announcement, Rodriguez noted, should draw increased attention to the case. "We believe that the combination of publicity, the significant reward, and the team of experienced investigators working the case from the Dallas Violent Crimes Task Force and the Irving Police Department will result in Said's arrest."

Special Agent Gil Balli, a task force supervisor who is leading the investigation, explained that "Said likely fled immediately after the murders. There have been many reports that he is in the U.S., but we are not ruling out the possibility that he is abroad." Balli added that investigators are coordinating with law enforcement partners in Egypt and Canada along with U.S. law enforcement agencies.

The last confirmed sighting of Said, now age 57, was in Irving, Texas, in 2008. He is 6 feet 2 inches tall, weighs about 180 pounds, and has brown eyes, black hair, and possibly a thick moustache.

Digital billboards featuring new FBI Top Ten Fugitive Yaser Abdel Said are being displayed nationwide.

In addition to Egypt and Canada, investigators believe Said has ties to the Dallas-Fort Worth region and the New York City area. He frequents diners—including Denny's and IHOP restaurants—smokes Marlboro Lights 100s cigarettes, and loves dogs, especially tan- and black-colored German Shepherds. He may be working as a taxi driver.

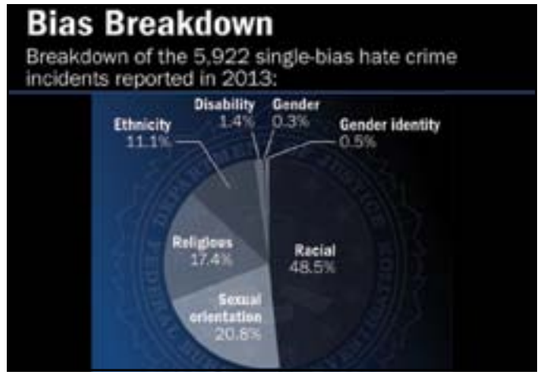
Said—the 504th person to be named to the FBI's Ten Most Wanted Fugitives list since its creation in 1950—is considered armed and dangerous. He reportedly carries a weapon with him at all times.

We need your help: If you have information about Yaser Abdel Said, call 1-800-CALL-FBI, or contact your nearest law enforcement agency or U.S. Embassy or Consulate. You can also submit a tip online at tips.fbi.gov.

"These murders were brutal and cold-blooded," Balli said. "If a person is capable of killing his own daughters, there is no telling what he might do. We need to catch this individual and prevent him from harming anyone else."

Note: Yaser Abdel Said may have been located since the above information was posted on our website. Please check our Ten Most Wanted Fugitives webpage at www.fbi.gov/wanted/topten for up-to-date information.

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



Latest *Hate Crime Statistics* Report Released

Publication Includes New Data Collected Under Shepard/Byrd Act

Today, the FBI released its annual *Hate Crime Statistics* report, which revealed that 5,928 hate crime incidents involving 6,933 offenses were reported by our law enforcement partners to the Bureau's Uniform Crime Reporting (UCR) Program in 2013. These hate crime incidents impacted a total of 7,242 victims—which are defined as individuals, businesses, institutions, or society as a whole.

The number of reported hate crimes last year is down slightly when compared to 2012 UCR figures—5,928 in 2013 versus the 2012 figure of 6,573 (a combination of the 5,796 incidents in *Hate Crime Statistics, 2012* and the 777 additional incidents published in *Hate Crime Addendum, 2012*).

Hate Crime Statistics, 2013—the first UCR publication to contain data collected under the Matthew Shepard and James Byrd, Jr. Hate Crime Prevention Act of 2009—has a few changes from previous reports. First, biases against gender (male or female) and gender identity (transgender and gender nonconformity) have been added to the list of bias categories. And in response to the Shepard/Byrd Act, we modified our data collection so that reporting agencies can indicate whether crimes were committed by, or directed against, juveniles.

Changes to this latest report include a revision of sexual orientation bias types, a revision of race and ethnicity categories, and the collection of rape data under the new UCR rape definition.

Left: Of the 5,928 hate crime incidents reported in 2013, 5,922 were single-bias offenses.

Among the report's findings for 2013:

- Of the 5,928 incidents reported, six were multiple-bias hate crime incidents involving 12 victims.
- Of the 5,922 single bias incidents reported, the top three bias categories were race (48.5 percent), sexual orientation (20.8 percent), and religion (17.4 percent).
- Of the reported 3,407 single-bias hate crime offenses that were racially motivated, 66.4 were motivated by anti-black or African-American bias, and 21.4 percent stemmed from anti-white bias.
- 60.6 percent of the reported 1,402 hate crime offenses based on sexual orientation were classified as anti-gay (male) bias.
- Law enforcement agencies identified 5,814 known offenders in the 5,928 bias-motivated incidents. Of these offenders, 52.4 percent were white and 24.3 percent were black or African-American.
- Of the 6,933 hate crime offenses reported in 2013, 63.9 percent were crimes against persons (e.g., intimidation, assaults, rapes, murders), while 35 percent were property crimes (mostly acts of destruction/damage/vandalism). The rest were considered crimes against society (like drug offenses or prostitution).

Upcoming changes to *Hate Crime Statistics*: The FBI approved a recommendation by the Criminal Justice Information Services Division's Advisory Policy Board to expand the bias types in the religious category to include all the religions identified by the Pew Research Center and the U.S. Census Bureau. Also, the hate crime data collection procedures will be modified to include an anti-Arab bias motivation. The collecting of both types of data will begin on January 1, 2015.

The UCR Program continues its efforts to assist our law enforcement partners in collecting and submitting hate crime data and with establishing or updating hate crime training programs for their personnel. Most recently, we held a training session for UCR contributors that focused on upcoming changes to the hate crime report, and we're in the process of revising our *Hate Crime Data Collection Guidelines and Training Manual* with new definitions and scenarios that reflect those changes.

A Commitment to Indian Country

Director Comey Pledges Continued Support for Crime Victims

At the 14th National Indian Nations Conference, which convened today on the reservation of the Agua Caliente Band of Cahuilla Indians in California, FBI Director James Comey pledged the Bureau's "unshakeable" commitment to tribal nations.

The Bureau has unique and important responsibilities in Indian Country, Comey told more than 1,000 conference attendees. Investigating crimes and assisting victims there, he said, "will be a priority of the FBI."

The conference, sponsored by the Department of Justice's Office for Victims of Crime and coordinated by the Tribal Law and Policy Institute, brings together Native Americans, community and government agencies, and service providers to share knowledge and develop programs to help those impacted by violence on tribal lands.

Comey noted that his interest in the FBI's Indian Country work is driven by his responsibilities as Director, but also by something more—his family. Last summer, his two youngest daughters went on a mission trip to a reservation and came home, he said, "with their eyes wide open about the challenges on the reservation. They said, 'Dad, you've got to do something, you've got to do more.'"

The FBI has investigative responsibility for 212 Indian reservations nationwide, and about 115 special agents work in our Indian Country program. Additionally, 41 victim specialists from our Office for Victim Assistance serve Native American crime victims. The Director acknowledged that those numbers should be higher.

To begin to address staffing and resource needs, Comey said, he has asked the Indian Country Crimes Unit and Office for Victim Assistance at FBI Headquarters to submit proposals detailing the need for increased staff, specialized training, and additional equipment.

Comey highlighted several areas in which the Bureau provides valuable resources to tribal nations:

- **Training.** Beyond the many training opportunities the FBI provides to tribal law enforcement, the Bureau is developing a new, three-week school—in partnership with the Bureau of Indian Affairs (BIA)—to equip new FBI and BIA agents, along with tribal law enforcement officers, with cutting-edge training on investigating Indian Country crimes.
- **Partnerships.** Currently, there are 14 Bureau-led Safe Trails Task Forces nationwide, bringing together federal, state, local, and tribal resources to combat violent crime, drugs, and corruption in Indian Country.
- **Victim assistance.** "Much of our work in Native American communities involves the most heartbreaking kinds of crimes—the homicides and the violent assaults and the rapes, and especially the abuse directed at kids," said Comey. FBI victim specialists provide on-scene crisis intervention and help victims and their families navigate the criminal justice process. "The work of our victim specialists is so important to the FBI that we made sure many of them were here today to meet with their counterparts in the BIA," explained Comey, "so they can talk with you about how to get better at their work."

Director Comey delivers remarks at the 14th National Indian Nations Conference.

"The essence of our job in the FBI," Comey added, "is to ensure that justice is done for everyone in America—every man, woman, and child living in any part of this great land—including American Indian and Native Alaskan communities."

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

Left: A badge from the Bureau of Investigation, as the FBI was called from 1909 to 1935, is seen on the left. At right is a 1917 photo of U.S. Attorney General Thomas Gregory, who served from 1914-1919. (Library of Congress Photo)

A Byte Out of History

The Bureau's Role During Early World War I Years

When war broke out in Europe a hundred years ago—in 1914, to be exact—the U.S. declared its neutrality, and U.S. investigative agencies like the Bureau of Investigation (the precursor to the FBI) had little role to play.

As the conflict escalated, though, American munitions, food, and other goods became a point of contention. Great Britain and its allies tried to purchase all they could afford from the U.S. to bolster their effort. But Germany and its allies, blockaded by British ships, took up submarine warfare to try and prevent their enemies from benefiting from American trade and turned to sabotage, espionage, propaganda, and other intelligence tactics to succeed.

The U.S. government's response was divided. On the one hand, the Treasury Department's Secret Service sought to pursue German spies and their agents in the U.S. In one well known case, a Secret Service agent tailing a known German agent in New York City picked up a briefcase accidentally left behind on a bus—it contained a trove of documents related to German efforts to clandestinely plan and support secret activities aimed at interfering with American assistance to the Allies.

On the other hand, because little of this activity violated the limited federal laws at the time, U.S. Attorney General Thomas Gregory cautioned the Bureau of Investigation to keep its investigations into German activities limited—even though they were potential threats to our national security.

That didn't mean the Bureau was on the sidelines, however. Between 1914 and American entry into the war in 1917, the Bureau's national security war-related investigations grew rapidly, from a small percentage of our total workload in 1914 to almost 30 percent two years later.

Among some of these early investigations:

- In 1914, Bureau agents broke up a ring run by Hans Adam Wedel, Carl Ruroede, and others who engaged in a variety of frauds to obtain passports for the use of German reservists stuck in the U.S. when war erupted.
- In 1915, Bureau agents investigated Werner Horn, a German national who bombed a bridge between Maine and Canada. Horn had attacked the Canadian side of the bridge and declared himself an agent of the German Army. The Bureau helped develop evidence that Horn had carried dynamite on public interstate transportation, a federal crime. He served 18 months in a U.S. prison and was later extradited to Canada, where he was sentenced for his sabotage.
- Also in 1915, agents in New York investigated a plot to blow up the Welland Canal, a major shipping point between Lakes Erie and Ontario. Paul Koenig, head of security for a German shipping line, and Richard Leyendecker, a New York antiques dealer, were arrested. German military attaché Franz von Papen was also charged for his role in the plot, but he had already left the U.S. by then. Papen, however, was soon connected to the previously mentioned Secret Service investigation involving a briefcase full of sensitive German documents left on a New York City bus.

In fact, it was these investigations by the Bureau and the Secret Service, along with Germany's resumption of unlimited submarine warfare and their plan to convince Mexico and Japan to ally with it against the United States, that helped convince America to enter the war on the Allied side on April 6, 1917.

That development brought even more work for the Bureau, as we will see in an upcoming story.

The Fraudster Who Faked His Own Death

Inside the Aubrey Lee Price Case

When a federal judge recently sentenced Aubrey Lee Price to 30 years in prison for bank fraud, embezzlement, and other crimes, it closed a chapter on the once successful businessman's sensational criminal saga.

Price went from a devout Christian minister and trusted financial adviser to a schemer who wiped out many of his clients' life savings and then faked his own death to avoid taking responsibility for what he had done. When a routine traffic stop in Georgia resulted in his arrest on New Year's Eve in 2013, Price acknowledged that he had become a drug dealer.

His well-publicized rise and fall makes for a fascinating tale, but our agents who investigated the case are quick to point out that the real focus of this story should not be on Price but rather on his victims.

"It's unbelievably sad," said Special Agent Ed Sutcliff in our Atlanta Field Office. "Most of Price's victims had worked 30 or 40 years to save for retirement. They were living off those funds," said Sutcliff, who interviewed many of the victims. "They had to learn from us that Price was missing, and all their money was gone."

Price told investigators he got involved in the investment business to help fund his mission efforts overseas. He worked for two well-known investment firms and later started his own company, PFG. Many of his clients were personal friends from Georgia, where Price lived. Some knew him from church—he gave seminars on how to be a wise Christian investor. Others had been on mission trips with him. Eventually, he consolidated PFG to about 100 "significant investors," Sutcliff said.

In 2009, unbeknownst to his clients, Price began gambling with their money, making risky investments. He would later falsify documents to hide those transactions. The following year, he convinced 40 of his clients to invest in a troubled Georgia bank and profit by turning the bank around.

Price raised $10 million from PFG clients, and bank employees and area residents put in $4 million. Price—who by this point was on the bank's board of directors—was seen as a hero for helping to keep it afloat.

But in 2011, Sutcliff said, Price realized the bank could not be turned around and that his investors stood to lose

When he was arrested on New Year's Eve day in 2013, Aubrey Lee Price had been on the run for nearly 18 months. To manage his life as a fugitive, Price created fake ID cards for himself like the ones shown here.

"a lot of money." He convinced bank officials to use some of the institution's funds to invest in U.S. securities and was permitted to wire $5 million to an account he said he created with a well-known global investment firm.

"Everyone believed Price was on the up and up," Sutcliff said. "He had investors, a solid track record, and there was no reason to doubt his ability or his honesty. And keep in mind that his PFG investors were getting bogus statements saying they were making money—and when they needed funds, he would provide them. It was the classic Ponzi scheme."

There never was an account with the global investment firm, and that initial $5 million was just the beginning of Price's thefts from the bank. He eventually gained access to more than $21 million and lost more than $16 million through risky investments—all the while telling the bank the money was being used to purchase securities. In the end, Price's deception resulted in the bank's failure and losses of more than $70 million.

In 2012, when he knew his house of financial cards was about to crumble, Price faked his suicide on a boat in Key West, Florida and fled first to Mexico and later to Florida, where he grew and sold marijuana and other drugs, and sometimes served as a bodyguard for prostitutes.

"He went from clean-cut preacher and investment adviser to weed grower and prostitute escort," said Sutcliff, who spent many hours interviewing Price. "He will tell you he made all those risky investments trying to earn back his clients' money," Sutcliff said.

"Like any good con man," Sutcliff added, "you want to believe what he is saying is true. But in the end, the words don't match the actions."

FBI Releases Expanded Crime Statistics for 2013

Latest Report from National Incident-Based Reporting System

Today, the FBI's Uniform Crime Reporting (UCR) Program released its third annual compilation of statistics from the National Incident-Based Reporting System (NIBRS), providing expanded data on more than 4.9 million criminal incidents reported to law enforcement in 2013.

The NIBRS, implemented to improve the overall quality of crime data collected by law enforcement, captures details on each single crime incident—as well as on separate offenses within the same incident—including information on victims, known offenders, relationships between victims and offenders, arrestees, and property involved in the crimes. In this latest report, 6,328 NIBRS agencies—about a third of the more than 18,000 law enforcement agencies that participate in the UCR Program—reported 4,927,535 crime incidents involving 5,665,902 offenses, 5,980,569 victims, 4,517,902 known offenders, and 1,533,671 arrestees.

While these numbers are not yet nationally representative, the FBI is undertaking a number of efforts to educate law enforcement and others on the benefits of the NIBRS and to increase participation in the program. For example, we have partnered with the Department of Justice's Bureau of Justice Statistics on the National Crime Statistics Exchange to assist states and agencies interested in submitting their crime data through the NIBRS.

As compared to UCR's traditional Summary Reporting System currently used in the annual *Crime in the United States* report—which is an aggregate monthly tally of crimes—the NIBRS is a more comprehensive accounting of crime occurring in a law enforcement agency's jurisdiction. When used to its full potential, the NIBRS can identify with precision when and where crime takes place, the form it takes, and the characteristics of its victims and perpetrators. Armed with this information, law enforcement agencies can better define and articulate the resources they need and then apply these resources where they'd be most effective.

When the UCR Program studied several years of NIBRS data to examine the effect of agencies switching to the system, most figures stayed the same—especially for the single-offense incidents—but slight increases occurred for agencies that had several multiple-offense incidents. For NIBRS submissions, all of the offenses in an incident were reported—not just the most serious one as is done in the Summary Reporting System. **So when agencies switch to the NIBRS, it may seem like crime within their region has increased, but that perception of an increase is due to the greater level of reporting specificity in NIBRS data compared to that for summary data.**

New in the NIBRS this year: This latest report includes information about new collection standards—and new data—including a revised rape definition, the addition of human trafficking offenses and gender and gender identity bias categories, and the revision of sexual orientation bias types and race and ethnicity categories.

Next year—at the request of the National Sheriffs' Association and the Animal Welfare Institute—an animal cruelty offense category will be added to the NIBRS and will include four separate types of abuse: simple/gross neglect, intentional abuse and torture, organized abuse (dog fighting and cock fighting), and animal sexual abuse. This new category will be implemented during 2015, and data collection will begin January 2016.

Digital Billboard Initiative

Catching Fugitives in the Information Age

In April 2013, a Buffalo grand jury indicted 33-year-old Oscar Romero and other suspected members of the Loiza Boys gang, charging them with heroin and cocaine distribution. After nearly a year on the run, investigators received information that Romero had returned to the Buffalo area from Puerto Rico, and the FBI deployed a powerful weapon to help capture the fugitive—digital billboards. The electronic billboards featuring Romero's face—along with the words "Wanted" and "Drug Charges" and a number to call—were posted in the Buffalo area on March 31, 2014. Four days later, Romero turned himself in.

"When our billboards went live, Oscar Romero had been a federal fugitive for just shy of a year," said Brian Boetig, special agent in charge of the FBI's Buffalo Division. "Our partnership with the local billboard company generated media attention and conversations throughout Romero's West Side neighborhood, which pressured him into safely surrendering."

Similar events have occurred around the country, thanks to the FBI's National Digital Billboard Initiative, which began in 2007 in Philadelphia when a graduate of the FBI's Citizens Academy—who happened to be an executive with Clear Channel Outdoor—offered to provide free space on the company's digital billboards to help catch criminals and rescue missing children.

Since then, the program has recorded impressive growth—and results. To date, the FBI has captured 53 individuals as a direct result of billboard publicity, and the Bureau now has access to more than 5,200 billboards nationwide made available by a number of companies. The billboard initiative is an excellent example of how law enforcement, the private sector, and the public can all work together to bring criminals to justice in today's information age.

"We view the partnership with the FBI as a model of public service," said Nancy Fletcher, president and CEO of the Outdoor Advertising Association of America (OAAA). "The billboard program makes a difference, using the latest technology on behalf of public safety."

The FBI has formal partnerships with OAAA, Clear Channel Outdoor, Lamar Advertising Company, Outfront Media (formerly CBS Outdoor), Adams Outdoor Advertising, the Fairway Media Group, CEMUSA, and the Outdoor Advertising Association of Georgia. All these organizations—including other digital advertisers who informally support the program—have been critical to the success of numerous investigative efforts, because digital billboards are extremely effective in reaching the public with information about fugitives, missing persons, and public safety issues.

Fugitive Daniel Andreas San Diego, wanted in connection with domestic terrorism, has been featured on a billboard in New York City's Times Square.

"The companies' willingness to assist us in bringing criminals to justice, as well as the speed in which they are able to publicize the information, is a tribute to their organizations," said Mike Kortan, assistant director for the FBI's Office of Public Affairs. "Their efforts have given us an added edge to identify, locate, and apprehend fugitives—and that, in turn, has helped to stop many criminals from further victimizing the public."

Because digital billboards can be quickly changed and updated, information about a kidnapped child, a bank robbery, or a matter of public safety can immediately be displayed. And messages can be targeted to specific geographic locations, which is important when time is of the essence.

And as the program expands, we are adding new formats. Fugitive information, for example, is now being displayed on digital bus shelters in Washington, D.C., and digital newsstands in New York City. "Thanks to our partnerships, the billboard initiative has been a tremendous success," Kortan said. "We look forward to its continued growth."

Most Wanted Talent

FBI Seeking Tech Experts to Become Cyber Special Agents

Since its earliest days, the FBI has looked for recruits with specialized skills to fill its special agent ranks: lawyers, accountants, scientists, and engineers, to name a few. Today, however, the most sought-after candidates possess a uniquely 21st century quality: cyber expertise.

Investigating cyber crimes—such as website hacks, intrusions, data theft, botnets, and denial of service attacks—is a top priority for the FBI. To keep pace with the evolving threat, the Bureau is appealing to experienced and certified cyber experts to consider joining the FBI to apply their well-honed tradecraft as cyber special agents.

"The FBI seeks highly talented, technically trained individuals who are motivated by the FBI's mission to protect our nation and the American people from the rapidly evolving cyber threat," said Robert Anderson, Jr., executive assistant director for the Bureau's Criminal, Cyber, Response, and Services Branch. "What we want are people who are going to come and be part of a team that is working different, very complex types of investigations and to utilize their skillsets in that team environment."

The Bureau recently launched a campaign to bring aboard more technical talent, including computer scientists, IT specialists, and engineers. In a job posting—open until January 20—the FBI says no other organization will apply the expertise of successful candidates like the FBI.

"One thing that no one else can offer is the mission and the camaraderie and the teamwork the FBI brings to the table," Anderson said. "Cyber agents will be integrated into all the different violations that we work. So whether it's a counterterrorism or counterintelligence investigation, they could be the lead agent in the case."

Key requirements to be a special agent include passing a rigorous background check and fitness test. Agents must be at least 23 and no older than 37. Prospective cyber special agents are expected to meet the same threshold as special agents, but also have a wealth of experience in computers and technology. Preferred backgrounds include computer programming and security, database administration, malware analysis, digital forensics, and even ethical hacking. An extensive list of sought-after backgrounds and certifications can be seen on the job posting.

"Cyber permeates every aspect of what we do," Anderson said. "That's why these types of people are so important to get into the pipeline and come into our organization."

Bank robberies help illustrate how the landscape has shifted. Traditionally, a team of agents responding to an armed bank robbery would cordon off a crime scene, interview witnesses, and collect evidence, such as fingerprints and security video. However, if the money was stolen through a cyber intrusion into the bank's holdings, the approach would be very different: a cyber agent would request firewall logs and forensic copies of hard drives, in addition to interviews.

The FBI already has a lengthy track record fighting cyber crimes. In June, the FBI announced its role in the multinational effort to disrupt the GameOver Zeus botnet, believed to be responsible for the theft of millions of dollars from businesses and around the world. A month earlier, the FBI announced charges against distributors of malicious software that infected millions of computers. Forty FBI field offices executed more than 100 search warrants and seized more than 1,900 domains used by Blackshades users to control victims' computers.

But the FBI wants to grow to meet tomorrow's challenges. "We're looking to hire a lot of cyber agents now," Anderson said. "It's an area where the FBI and the whole U.S. government will be looking for this talent for years to come."

Cyber agents can expect continued specialized training once onboard and to work on some of the Bureau's most complex cases. Given the broad scope of the FBI's work, Anderson says, "there is no other place like it."

FOREIGN COUNTERINTELLIGENCE

Index

HISTORY

INTELLIGENCE

INTERNATIONAL

MAJOR THEFTS/VIOLENT CRIME

ORGANIZED CRIME/DRUGS

PARTNERSHIPS

PUBLIC/COMMUNITY OUTREACH

PUBLIC CORRUPTION

RECRUITING

TECHNOLOGY

TRAINING

WHITE-COLLAR CRIME

Index

FBI OFFICE OF PUBLIC AFFAIRS
935 Pennsylvania Avenue NW
Washington, D.C. 20535

An FBI Miami Division diver comes up from the weed-infested waters of a pond in Florida during a cooperative search with FBI Jacksonville's Evidence Response Team.