Here is the evidence from FY 2010.
We are the primary federal law enforcement and security arm of the U.S. Postal Service.

Our Postal Inspectors investigate criminals who fraudulently misuse the U.S. Mail to commit crime.

Here is the evidence from FY 2010.
The Ponemon Institute in FY 2010 ranked the U.S. Postal Service in first place as the “Most Trusted Government Agency” for an impressive sixth year in a row. It also analyzed the privacy practices of America’s largest brands and ranked the Postal Service among its top 10 businesses as the “Most Trusted Company for Privacy” the sixth year in a row it received that rating.

We’re part of the reason why.
EXECUTIVE COMMITTEE

Guy J. Cottrell
Chief Postal Inspector

Gregory Campbell, Jr.
Deputy Chief Inspector
Western Field Operations

R. Emmett Mattes III
Chief Counsel

Randy S. Miskanic
Deputy Chief Inspector
Headquarters Operations

Shawn S. Tiller
Deputy Chief Inspector
Headquarters

Teresa L. Thome
Deputy Chief Inspector
Eastern Field Operations
MESSAGE FROM THE CHIEF POSTAL INSPECTOR

This year’s Annual Report of Investigations of the United States Postal Inspection Service encapsulates all that is integral to the mission of this agency: supporting and protecting the U.S. Postal Service and its employees, infrastructure, and customers; enforcing the laws that defend the nation’s mail system from illegal or dangerous use; and ensuring public trust in the mail.

U.S. Postal Inspectors across the country safeguard every element of the postal system—including the hundreds of thousands of postal employees who process and deliver the mail and the millions of customers who use it. Postal Inspectors protect thousands of postal facilities and millions of dollars in postal assets—including vehicles, equipment, products, and revenue streams. In the past fiscal year, Postal Inspectors initiated more than 6,000 investigations and arrested over 6,000 suspects for crimes involving the mail or against the Postal Service.

The Postal Inspection Service continues to meet its overall goal of assuring the security of the Postal Service. About 46 percent of Inspectors’ arrests in FY 2010 related to mail theft—a total of 2,775 suspects. Postal Inspectors arrested approximately 1,000 suspects on mail fraud charges, and analysts prepared 76,955 responses to mail fraud complaints. Revenue-protection efforts by Postal Inspectors over the past year identified in excess of $110 million in postal revenue losses.

I was proud to attend a DOJ press conference this past year with Attorney General Eric Holder and representatives from other law enforcement agencies to announce the results of Operation Broken Trust. Our contribution to this 3½-month sweep targeting fraudulent investment schemes covered 37 mail fraud cases, including 11 Ponzi schemes, affecting more than 36,000 postal customers who suffered $600 million in losses. Results like this demonstrate the viability of our work in increasing the trust and confidence of postal customers through our investigations of fraudulent activity involving the mail.

Inspectors protect even more customers by educating them about fraudulent schemes. In a brochure that was mailed to nearly every home in America, Postal Inspectors delivered information teaching customers how to recognize the warning signs of fraud. Inspectors know that when citizens understand how fraud schemes work, they avoid becoming victims. This nationwide consumer initiative was made possible by money collected in fines and damages from criminals convicted of fraudulent schemes.

Postmaster General Pat Donahoe says “The customer is the focus of everything the Postal Service does.” And that really defines all of the work we do.

Guy J. Cottrell
As one of our country’s oldest federal law enforcement agencies, founded by Benjamin Franklin, the United States Postal Inspection Service has a long, proud, and successful history of fighting criminals who attack our nation’s postal system and misuse it to defraud, endanger, or otherwise threaten the American public. As the law enforcement, crime prevention, and security arm of the United States Postal Service, the U.S. Postal Inspection Service is a highly specialized, professional organization performing investigative and security functions dedicated to ensuring confidence in the mail.

Congress empowered the Postal Service “to investigate postal offenses and civil matters relating to the Postal Service.” Through its security and enforcement functions, the Postal Inspection Service assures American businesses that they can safely dispatch funds, securities, and information through the U.S. Mail; postal customers that they can entrust their correspondence to the U.S. Mail; and postal employees that they will work in a safe environment.

As the Chief Security Officer for the U.S. Postal Service, the Chief Postal Inspector is responsible for issuing instructions and regulations on security requirements. Postal Inspection Service personnel conduct security reviews and collaborate with postal employees to bolster security countermeasures. Further, the Postal Inspection Service partners with other postal managers in efforts to attain strategic agency goals.

Postal Inspectors are federal law enforcement officers who carry firearms, make arrests, execute federal search warrants, and serve subpoenas. As fact-finding and investigative agents, Postal Inspectors work closely with U.S. Attorneys, other law enforcement agencies, and local prosecutors to investigate postal cases and prepare them for court. Postal Inspectors are stationed throughout the United States and enforce roughly 200 federal laws covering investigations of crimes that adversely affect or entail fraudulent use of the U.S. Mail and the postal system.
WHAT WE DO>

PROTECT

PREVENT

RESPOND
To assist in carrying out its responsibilities, the Postal Inspection Service maintains a Security Force of armed, uniformed Postal Police Officers, as well as contract security guards, who are assigned to critical postal facilities throughout the country. The officers provide perimeter security, escort high-value mail shipments, and perform other essential protective functions.

The Postal Inspection Service’s professional, technical, and administrative employees play a vital role in supporting the criminal investigative and security functions of the agency. They perform a wide variety of tasks, including facilitating direct communications with Congress, other postal groups, and the public. The agency’s national information technology infrastructure supports users at nearly 200 sites nationwide, and its offices are linked nationally via a private law enforcement network.

Postal Inspection Service staff issues news releases covering investigations and events of national interest and disseminates consumer-education publications with prevention advice on mail-related crime. They represent the agency’s interests on Capitol Hill and in cooperative activities with other government, law enforcement, and consumer agencies. The agency’s Internet Web site delivers news about its latest investigations and fraud alerts, and provides an online venue for postal customers to report suspected incidents of mail theft or vandalism, identity fraud, and mail fraud, while its Intranet facilitates confidential employee communications across the country.

The Postal Inspection Service extends full cooperation to all federal, state, and local investigative and prosecutive authorities in law enforcement matters to ensure greater protection for the public.

For more information on the Postal Inspection Service, visit postalinspectors.uspis.gov.
PROTECTING>

POSTAL PEOPLE
PERSONNEL SECURITY

The U.S. Postal Inspection Service is committed to ensuring safety in the workplace for postal employees. Threats originate both externally and internally, from sources including criminals bent on robbery, burglary and assault, malicious mailers of bombs or other dangerous substances, deranged and disgruntled individuals who mail threats, narcotics traffickers, pranksters, and agitated co-workers.
WORKPLACE VIOLENCE

Every business, whether it is a federal or state entity, in the private or nonprofit sectors, large or small, is susceptible to workplace violence. And like every business, the Postal Service has an obligation to provide its employees with a safe and secure place to work. Among the ways it meets this obligation is by implementing strategies proven to reduce workplace violence.

The Workplace Violence Prevention Program provides the tools and resources essential to teach prevention and response measures. Its underlying message supports the agency’s policy of “zero tolerance” for violence by or against its employees.

Zero tolerance means that every act or threat of violence, regardless of the initiator, elicits an immediate and firm response. The response could result in corrective action, up to and including removal of the offender from employment with the Postal Service. If all other measures have been exhausted, Postal Inspectors must step in. Their response could result in arrest and prosecution.

The Postal Service offers training for managers and supervisors in workplace violence awareness and has put in place Threat Assessment Teams (TATs) at each postal district. Postal Inspectors serve as core members to TATs, helping to assess situations, determine risks, and develop risk-abatement plans. Inspectors may also address violence-prevention issues in “stand-up talks” for employees at postal facilities, sometimes in conjunction with showing “Workplace Violence: Stop it Before it Happens”—a Postal Inspection Service-produced video that reinforces steps employees can take to resolve conflicts before they escalate to violence.

Here’s an example of a case investigated by Postal Inspectors during the reporting period:

In June a mail handler at the Postal Service’s International Service Center in New York grabbed his supervisor from behind, stabbed her with blunt-edged scissors, and struck her multiple times; Postal Police Officers and Postal Inspectors immediately responded to the scene. A Postal Inspector accompanied the supervisor to the hospital, where she was treated for lacerations and abrasions. Inspectors also arrested the mail handler, who told them “I got mad, so I stabbed her in the head” and provided a full written confession, stating he “had thought of killing her since October 2009 on and off for many different reasons.” He was charged with attempted murder, first-degree assault, and criminal possession of a weapon, and was removed from the Postal Service.
Assaults and Threats

Physical assaults on and threats against postal employees can occur during robbery attempts, but other attacks stem from personal motives and inexplicable behavior by disturbed individuals. No matter the motive, Postal Inspectors vigorously investigate every assault or threatened assault against postal workers.

The U.S. Postal Inspection Service is committed to ensuring employee safety in the workplace. Postal Inspectors investigated 508 postal-related assaults and credible threats during FY 2010—a 4.7 percent decrease from the 533 investigated in the previous fiscal year—and arrested 229 suspects. Criminal prosecution of offenders is one remedy Postal Inspectors use to deter assaults and threats against postal employees. Inspectors also work closely with postal managers to implement violence-prevention strategies.

Assaults & Threats: Two-Year Trend

<table>
<thead>
<tr>
<th>Year</th>
<th>Assaults and Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 09</td>
<td>533</td>
</tr>
<tr>
<td>FY 10</td>
<td>508</td>
</tr>
</tbody>
</table>

Here is a sampling of assault and threat cases Postal Inspectors investigated in FY 2010:

- The man who attacked, kidnapped, and sexually assaulted a letter carrier while she was delivering mail on her route was sentenced in August in Memphis, TN, to 20 years in prison and five years’ supervised release for assaulting a federal employee—the maximum allowable sentence—with a separate 25-year prison term and five years’ supervised release for kidnapping a federal employee. The suspect left the scene after the assault but returned a few seconds later to steal the carrier’s purse. Postal Inspectors learned a man whose description matched the suspect was seen fleeing the area. They arrested him the next day, and his DNA was matched with the victim’s rape kit sample.

- In May, Postal Inspectors arrested a former letter carrier on attempted murder charges after he rammed his former postal supervisor with a truck. The victim was walking from his car to report to work in Albany, CA, when the carrier—who was fired in December 2009—steered his truck into the supervisor, pinning him against his own vehicle, breaking his arm, and causing other injuries. When the supervisor tried to escape, the suspect backed up, attempted to hit him again, crashed into parked vehicles, and drove off. Inspectors responded to the scene and later arrested the attacker.

- A woman found guilty in the September 2008 beating of a letter carrier from the Washington Street Postal Station in Hartford, CT, was sentenced in February to five years in jail and three years’ supervised release. The attack apparently was motivated by a love triangle. The suspect approached the female carrier as she was delivering mail and viciously beat the carrier on the head with a hammer, causing serious physical injury. Inspectors responded immediately to the scene and canvassed the area for witnesses; along with postal supervisors, they also visited the carrier and her family in the hospital. Victim-witness coordinators provided counseling to the carrier, who later recovered from her wounds.
CAPTURING ROBBERS

Robberies not only pose a threat to postal employees, but also jeopardize the public’s trust in the mail and attack the financial integrity of the Postal Service. Robbers who accost letter carriers usually are seeking mail containing valuables—anything from financial information to checks, jewelry, or illegal drugs. They also rob carriers for personal property. Those who target Postal Service facilities are generally after cash, money orders, and stamps.

In FY 2010, the U.S. Postal Service experienced 75 robberies or attempted robberies of postal employees, Post Offices, and contractors. Postal Inspectors arrested 61 suspected robbers during that period and reported 43 convictions, some from cases in prior reporting periods.

Since the U.S. Mail and Post Offices likely will remain compelling targets for larceny, Postal Inspectors in all parts of the country receive expert training on how to safeguard employees and facilities against criminals. Inspectors actively educate employees on ways they can protect themselves on the job.

Postal Inspectors aggressively investigate all postal robberies and attempted robberies, such as these examples from 2010:

- In January, two armed suspects robbed a postal truck driver of two Registered Mail pouches shortly after the driver arrived at the Porter Square Finance Station in Cambridge, MA. Postal Inspectors visited Post Offices in the area to talk to employees about the robbery and distribute prevention information; they also handed out 1,000 fliers to letter carriers on nearby routes advertising a $50,000 reward, and posted fliers at bus stops, train stations, and local businesses. Resulting leads identified three suspects who were planning another robbery in March at the Charlestown Post Office. Inspectors conducted surveillance at Charlestown, arrested the men, and seized a handgun and masks. When Inspectors executed a search warrant at one suspect’s home, they seized additional weapons, a jacket used in the robbery, and
cocaine, and arrested the three suspects. The Boston U.S. Attorney’s Office accepted the case for prosecution.

- In March the man who robbed the Ampere Finance Station in East Orange, NJ, was sentenced to more than 15 years in prison and five years’ supervised release, and was ordered to pay $9,054 in restitution to the Postal Service. When he robbed the station at gunpoint in May 2009, he bound a postal employee with duct tape and made off with cash and checks. Postal Inspectors identified the man after developing several leads.

- A California man with two previous federal offenses was sentenced to 35 years to life in prison for the armed robbery and carjacking of a letter carrier from the Greenmead Station. Postal Inspectors’ pursuit of DNA evidence from a discarded cigar tip was critical in the conviction.

- A man arrested by Postal Inspectors pled guilty to the armed robbery of the Bullhead City, AZ, Highway Station and was sentenced to eight years in prison and five months of supervised release. Postal Inspectors and local police responded after a man entered the station, claimed to have planted a plastic explosive in the building, held a gun to the head of the clerk, and escaped with cash and postal money orders.

ARRESTING BURGLARS

Burglars continue to target postal facilities in hopes of stealing cash or money orders. In FY 2010, Postal Inspectors reported 129 burglaries at postal facilities nationwide—but due to increased security and aggressive investigations, these crimes resulted in only minor losses. Postal Inspectors arrested 62 suspected burglars in FY 2010 and reported 51 convictions from cases originating in this and prior reporting periods.

These postal burglaries illustrate Postal Inspectors’ challenges in protecting Postal Service revenue:

- When the Conley, GA, Post Office was burglarized on March 24 and April 17, video surveillance collected images of a masked suspect entering the building, removing door locks, moving the surveillance camera, and stealing property. On April 30, cameras again captured images of the suspect driving up to the Post Office, cutting the gate lock, entering the building, and stealing property. They also captured an image of the man removing his mask and of the license plate on his vehicle. Inspectors identified him as a former postal employee. When they arrested him, he confessed to burglarizing the Conley Post Office three times and the Rex Post Office once.

- In April 2010, a man suspected in the burglary and arson of the Stark, KS, Post Office was sentenced to five years in prison and five years of supervised release. He also was ordered to pay $3,600 in restitution to the Postal Service for damages caused to the Post Office when he set fire to the building to cover his tracks. The suspect currently is serving 15 years in the Kansas Department of Corrections on unrelated charges. His federal sentence will run concurrently with his state sentence.
What the Postal Inspection Service refers to as “dangerous mail” is any mail containing biological, chemical, radiological, or potentially explosive substances. Postal Inspectors receive specialized training and equipment to address the threats these substances can pose to postal employees, to postal customers, and to the mail system. Inspectors partner with officials from other agencies in the homeland security community and with representatives of national security programs and intelligence groups to offer mobile-mail screening at events of national significance and to maximize resources, lend guidance, and share best practices.

Postal Inspectors employ tested protocols for, and coordinate responses to, reports of alleged or suspected dangerous items related to the mail or found at mail facilities. Inspectors respond to suspicious mail incidents, resolve alleged and actual threats, and investigate all incidents and related criminal activity as needed.

The Postal Inspection Service’s mail-screening program has proven to be effective for postal employees, customers, and the Postal Service. While the majority of dangerous mail incidents are found to be nonhazardous substances or items, an immediate response by Postal Inspectors not only assures employees of a safe and secure workplace, but also ensures that postal facilities can continue operations rather than be shut down for needless and alarming evacuations. The result is fewer lost workhours, greater productivity, and improved service to customers.

FY 2010 statistics tell a story of success: Postal Inspection Service efforts reduced lost workhours by 14.8 percent from the previous year. Inspectors’ actions also reduced delayed mail—and lowered operating costs associated with evacuations. And Postal Inspectors’ interventions limited the number of unnecessary requests for disaster services, freeing local first responders for other emergencies.

In FY 2010, the Dangerous Mail Investigations Group recertified Postal Inspectors to meet the requirements of the Occupational Safety and Health Association for hazwoper certification, administering quality assurance and refresher exercises. Inspectors also delivered 945 educational seminars over the past year to employees, business owners, and other law enforcement and government agencies addressing mail safety and handling protocols.

While the number of incidents remained high, lost workhours caused by reports of suspicious items or substances decreased by 49% since FY 2008—the result of proper training for postal employees in response protocols and new screening practices and equipment for Postal Inspectors.
Suspicious Substances in the Mail

Postal Inspectors respond rapidly to ensure early detection when unidentified substances in the mail or threats involving chemical, biological, or radiological material are reported. Not all incidents involve criminal intent, but a rapid response ensures that Postal Inspectors are on the scene whenever mail is used to convey dangerous substances.

Postal Inspectors trained as Dangerous Mail Investigations Specialists use specialized screening equipment and deploy established threat-assessment protocols to respond when suspicious substances are suspected in mail or at mail facilities. They determine whether the substances are hazardous and could threaten postal employees, customers, or facilities.

In FY 2010, Postal Inspectors responded to 2,269 incidents nationwide involving unidentified suspicious powders and liquids reported by postal employees, customers, or other federal agencies. The unidentified substances were found in the Postal Service’s critical infrastructure, at postal facilities, or in U.S. Mail.

Here are some cases Postal Inspectors investigated in the past fiscal year:

- Postal Inspectors arrested a man in October 2009 for mailing threatening letters containing a suspicious powder to a federal judge. The letters demanded $1 million in cash in exchange for the safety of the judge and his family. Inspectors tracked down the man after determining that two of the stamps on the letters had been purchased at the Goodlettsville, TN, Post Office. The man confessed he wanted to scare the judge, who he felt had given him a harsh sentence in a previous case. For this crime he was sentenced to five years in prison and three years of supervised release. The judge described his actions as disturbing and highly terroristic.

- A man pled guilty in August to federal charges of mailing threatening communications and white powder. Postal Inspectors proved he was responsible for mailing 26 letters to the President, elected government officials, foreign embassies, consulates, and private citizens throughout the United States. His mailings contained handwritten threats and a suspicious powder, and several cited health care reform, also noting: “Take a whiff of this.”

Suspicious Items in the Mail

Postal Inspectors respond to reports of suspicious items such as improvised explosive devices (IEDs)—commonly called mail bombs—that are placed in the mail or on postal property. Fortunately, mail bombs are exceptionally rare.

If a mail bomb detonates, the life and safety of those in the vicinity of the explosion are the first priorities for Postal Inspectors and other responders. Postal Inspectors also secure the crime scene and process the area for evidence.

Mail Bomb Incidents: Five-Year Trend

<table>
<thead>
<tr>
<th></th>
<th>FY 06</th>
<th>FY 07</th>
<th>FY 08</th>
<th>FY 09</th>
<th>FY 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCIDENTS</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>EXPLOSIONS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>INJURIES</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>DEATHS</td>
<td>none</td>
<td>none</td>
<td>none</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

In FY 2010, Postal Inspectors responded to 1,085 incidents involving explosive devices placed in mail receptacles, hoax bombs, suspicious items found in postal facilities or equipment, and mailed explosive devices. Most of the incidents involved false alarms or items inadvertently left behind by customers; the remainder involved hoax devices or homemade explosives used to vandalize mailboxes. Postal Inspectors investigate even the threatened use of dangerous materials in the mail.
Following are examples of Postal Inspectors’ investigations in the past fiscal year:

- Postal Inspectors arrested a man after they observed him planting a bomb in a postal collection box. He was accused of placing 36 explosive devices—both pipe bombs and Molotov cocktails—in East Texas over six months. Twenty-three of the devices were placed at 16 postal-related sites, mainly collection boxes. He told Inspectors he was upset with the way government agencies handled a 25-year-old case in which he was defrauded of a large monetary settlement.

- Postal Inspectors arrested a man in Marmet, WV, in July 2009 for mailing an IED to his former neighbor in Houston, MN. When the victim opened the parcel, he thought the contents looked unusual so he notified local law enforcement; an IED concealed inside was set to detonate when opened. The victim believed his former neighbor might have mailed the IED because of a past dispute. When interviewed by Postal Inspectors, the suspect admitted to mailing the device as a scare tactic. He was sentenced to two and one-half years in prison and three years’ supervised release.

- Postal Inspectors were notified in September 2009 that an IED had exploded when an employee at a business in Visalia, CA, opened a parcel sent via the mail. When the victim opened a tackle box inside the package and removed some of the packing, he saw five PVC pipes with end caps; one of the pipes exploded, causing lacerations and flash burns across his arms. Postal Inspectors identified a suspect who was indicted in October for mailing the explosive device.

### Restricted and Prohibited Mail

Mail that contains harmful or dangerous material is considered non-mailable, either by federal statute or by postal regulation. The basic premise of postal mailable statutes is that anything “which may kill or injure another, or injure the mail or other property...” is non-mailable.

Restricted material includes any article or substance prohibited or limited by Title 18 of the U.S. Code—such as liquor, items emitting obnoxious odors, liquids, powders, or battery-powered devices. It also pertains to hazardous material, such as poisons, ammunition, firearms, or explosives. Postal employees may refuse an article for mailing if the content of the article is described by the mailer or otherwise revealed to be non-mailable.

In FY 2010, Postal Inspectors responded to 187 incidents nationwide involving restricted, hazardous, or otherwise non-mailable material found in the mail or at postal facilities.

Inspectors’ case examples from the reporting period follow:

- A man was sentenced in March for mailing three AK-47 machine guns from Iraq, where he worked for a security contractor, to his home in Dublin, VA. Inspectors seized the weapons before they were delivered.

- A man was sentenced in federal court in December 2009 to two years in prison and two years’ supervised release for dealing firearms without a license. Postal Inspectors found the man had shipped 20 handguns with obliterated serial numbers via the U.S. Mail to the U.S. Virgin Islands from Ft. Lauderdale, FL.
Postal Inspectors work hard to ensure the mail is safe for handling by postal employees and customers—and they seize from the mailstream any items containing harmful or dangerous material. In Puerto Rico last year, Inspectors seized 105 guns sent illegally through the U.S. Mail.
Mail Screening at National Special Security Events

Public gatherings may be viewed as attractive targets for terrorists due to the publicity they can generate or because of their political connection. When they are designated as National Special Security Events, Postal Inspectors are requested to participate as valued partners who convey an “envelope of safety” by protecting mail delivered to these high-profile venues.

The Postal Inspection Service’s mail-screening program supports Postal Service mandates related to Department of Homeland Security (DHS) Presidential Directives. As described in the DHS National Response Plan, the Postal Inspection Service was named to the DHS Special Events Working Group to provide subject-matter expertise in chemical, biological, radiological, and explosives incidents. Inspectors have conducted mail-screening for presidential and political events, the Olympic Games, Super Bowls, and various dignitary conventions.

Postal Inspectors screened mail at 12 events in the past fiscal year, including the 2010 Super Bowl, Nuclear Security Summit, and National Governors’ Conference. Senior Technical Surveillance Specialists accompany Inspectors at these events to ensure proper equipment maintenance and operation.

Integral to the mail-screening program is the Postal Inspection Service’s Mobile Mail-Screening Station, a transportable, self-contained platform that provides mail screening for chemical, biological, radiological, and explosive threats. The Postal Inspection Service also deploys specially-equipped vans that contain X-ray units and field-screening equipment.

The Postal Inspection Service provided security for mail and mail-related matter at selected sites and investigative and intelligence support during these events. Postal Inspectors coordinated mail-screening for the four largest carriers: the Postal Service, United Parcel Service, FedEx, and DHL International. They also conducted mail-screening for smaller messenger and courier services along with U.S. Secret Service agents.

The Canadian Government’s Department of Foreign Affairs and International Trade requested that Postal Inspectors screen all mail and packages destined for the Vancouver 2010 Olympics from January 25 through March 19. Inspectors screened a total of 33,278 mailpieces during the operation.

Postal Inspectors assigned to these events performed their duties as part of their work with the FBI’s National Joint Terrorism Task Force and its Intelligence Operations Center, as well as with DHS’s National Operations Center.
IMPEDEING NARCOTICS TRAFFICKING

The U.S. Postal Inspection Service interdicts mailings of illegal drugs and drug proceeds and investigates organized narcotic distribution groups to protect employees and customers from the violence related to drug trafficking and to preserve the integrity of the U.S. Mail. Postal Inspectors, often working with other law enforcement officials, arrested 1,322 suspects for drug trafficking via the mail in FY 2010. Their investigations resulted in the seizure of approximately $7.6 million in cash and monetary instruments, and 37,759 pounds of illegal narcotics found in the mail.

Drug Mailings in South Texas

Illegal drug mailings from South Texas—identified as a problem for several years running—continued to rise in FY 2010. By the end of the fiscal year, Postal Inspectors in McAllen had interdicted 3,364 parcels, a whopping 44 percent more than those seized only one year earlier; they attribute the rise to trafficking by Mexican drug cartels. Inspectors in Texas staged numerous interdictions of the mail, seizing 20,020 pounds of marijuana and arresting 39 marijuana mailers.

South Texas Marijuana Mailings Seized: Five-Year Trend

<table>
<thead>
<tr>
<th></th>
<th>DRUG PARCELS</th>
<th>POUNDS OF DRUGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 10</td>
<td>3,364</td>
<td>20,020 lbs.</td>
</tr>
<tr>
<td>FY 09</td>
<td>1,759</td>
<td>19,380 lbs.</td>
</tr>
<tr>
<td>FY 08</td>
<td>699</td>
<td>7,010 lbs.</td>
</tr>
<tr>
<td>FY 07</td>
<td>303</td>
<td>3,471 lbs.</td>
</tr>
<tr>
<td>FY 06</td>
<td>221</td>
<td>2,310 lbs.</td>
</tr>
</tbody>
</table>

Here are some examples of Inspectors’ work in the past fiscal year:

- Postal Inspectors identified a man in Houston who had been mailing marijuana to 10 states since 2006. Inspectors linked at least 89 Express Mail packages weighing more than 900 pounds to the suspect; they arrested him in August and he now faces federal charges. Under federal warrant, Inspectors seized numerous Express Mail receipts, postal scales, and packing materials from the suspect and determined he was receiving drug payments via Express Mail.

- Postal Inspectors investigated a suspected marijuana trafficker after letter carriers in Queens, NY, reported being harassed by individuals looking for drug mailings. Inspectors identified (and later arrested) two letter carriers who they found were collaborating with organized rings to help deliver the drugs. Inspectors also identified a dealer in Arizona who was paying others to mail the marijuana to New York. Inspectors went after the source of the supply, resulting in seven arrests and the seizure of two handguns, an AK-47 assault rifle, a Cadillac SUV, and $28,000 in cash. The main defendants are a father and son who are well known to state and federal authorities in Arizona as suspects in multiple investigations, but who had managed so far to elude prosecution. Not this time: In August the father and son were convicted in federal court and sentenced to 10 and 12 years in prison, respectively.

- In 2007 Postal Inspectors in New Jersey and Puerto Rico advised Inspectors in Laredo, TX, that they had seized Express Mail parcels containing marijuana mailed from Laredo, and postal money orders used to launder drug proceeds. Experts at the Postal Inspection Service’s National Forensic Laboratory helped to identify the mailings and the money orders, finding that ring members used U.S. Mail, pri-
marijuana from Texas to New Jersey, Puerto Rico, Minnesota, and Florida. Inspectors linked the ring to 17 Express Mail parcels containing about 164 pounds of marijuana; ring members had also laundered more than $1.2 million in drug proceeds, including about $262,495 in postal money orders. Postal Inspectors have since attributed 75 other parcels to the ring. Inspectors arrested five suspects; four pled guilty and were convicted over the past year, and prosecution is pending for the remaining suspect.

**Fusion Center of the Organized Crime Drug Enforcement Task Force**

The Organized Crime Drug Enforcement Task Force (OCDETF) is a multi-agency partnership of federal, state, and local law enforcement officers who share information and intelligence to identify, disrupt, and dismantle drug-trafficking rings and their related money laundering activities.

OCDETF created the Fusion Center in 2004 to centralize intelligence from these groups, which, in addition to the Postal Inspection Service includes ATF, FBI, DEA, ICE, IRS, Coast Guard, DOL-Office of Inspector General, Customs and Border Protection, State Department, U.S. Marshals Service, Secret Service, Financial Crimes Enforcement Network (FinCEN), and the National Drug Intelligence Center.

Fusion Center activities greatly benefit the Postal Inspection Service by supplying timely intelligence needed for investigations of illegal drugs, money laundering, organized crime, and other offenses that can adversely affect Postal Service employees, customers, resources, operations, and service. Through information sharing and monitoring, the Fusion Center ensures that agency investigations do not conflict with one another. The center assists in developing investigative leads and boosts agencies’ investigative resources through in-depth analyses of the financial and organizational structures of major criminal organizations.

In FY 2010 Fusion Center staff furnished 183 reports to Postal Inspectors. Eight postal employees were identified as subjects of investigations by other federal agencies and were referred to the Postal Inspection Service for investigative attention.
PROTECTING POSTAL INVESTMENTS
ASSET SECURITY

U.S. Postal Inspectors daily confront diverse threats to Postal Service assets: dishonest mailers and counterfeiters siphon postal revenues, burglars target postal facilities, and businesses hoard postal property for private use. The Postal Inspection Service, constantly vigilant in preventing and pursuing these schemes, is essential to the financial viability of the Postal Service. Besides investigating fraud and crime targeting the Postal Service, Postal Inspectors proactively protect postal facilities and operations by conducting security reviews and upgrading security systems and procedures.
**SAFEGUARDING REVENUE**

The Postal Inspection Service formulated its Revenue Investigations Program as a safeguard for Postal Service revenue, designed not only to protect postal revenue from criminal attack but also to assure the integrity of products and services for postal customers. Postal Inspectors must continually evaluate products and revenue systems for the many postage and service options used by the public. They devise specialized prevention and investigative strategies to safeguard areas posing the highest risks for loss.

Postal Inspectors measure the effectiveness of their revenue investigations by the number and types of schemes they identify and by how many they successfully resolve. In addition to stopping fraud, resolutions may involve criminal or civil prosecutions, recovery of lost funds and, in some instances, the collection of fines and penalties.

**Reducing Financial Risks**

Postal Inspectors launched an initiative in FY 2010 aimed at evaluating internal financial controls and risks at business mail entry units (BMEUs)—areas of postal facilities where large quantities of mail are received from customers, verified, documented, and processed.

The reviews tested key controls at 108 BMEUs as set by the Sarbanes-Oxley Act (SOX) Compliance Group of the Postal Service, as well as controls indicated as vulnerable by Inspectors’ investigations. Postal Inspectors not only reported their results to the SOX Compliance Group but also are using the
Each year, the Postal Service spends millions of dollars to replace pallets that leak out of its network. USPS provides pallets to mailers for bulk shipments, but far too often, they’re not returned. With wooden and plastic pallets ranging from $7 to $20 each, losses quickly add up. In FY 2010, Postal Inspectors recovered more than 21,000 pallets and other postal equipment with an estimated value of close to $1.75 million.
data to form a new initiative that will protect revenue and evaluate risks for presort mail. Presort mail is favored by high-volume mailers who qualify for discounts when they present mailings sorted to specific standards.

Postal Inspectors conceived a plan to implement controls by assessing risk based on input from Postal Service managers and by reviewing Inspectors’ criminal cases tied to BMEUs. They developed the BMEU Risk Assessment for Inspector use in the field, with guidelines for reporting, collecting, and analyzing data. Nationwide training sessions required Inspectors at the 18 major division offices to complete six BMEU Risk Assessment reviews by the end of the fiscal year.

Following a BMEU Risk Assessment in June, Postal Inspectors arrested a Passaic County, NJ, employee for stealing $384,000 from accounts held by the county superintendent of elections. The confidential secretary for the superintendent oversaw numerous permit imprint accounts at Post Offices across northern New Jersey. Inspectors learned she deliberately overfunded the accounts and then submitted requests for refunds; over a two-year period she submitted 16 refund requests to the Postal Service and received back about $270,000, which she deposited into her own bank accounts. Inspectors learned she had also intercepted and altered another $110,000 worth of checks mailed to the election supervisor by townships in Passaic County for reimbursement of voting machine rentals and election costs.

Investigating Revenue Fraud

The Postal Service derives a large portion of its revenue—nearly 50 percent—from permit imprint mail, which represents one of the agency’s most vulnerable areas of revenue risk. Permit imprints are convenient for high-volume mailers, who print required information in a block at the upper-right side of each mailpiece rather than apply individual postage or meter stamps.

Along with staff from the office of Intelligent Mail and Address Quality, Postal Inspectors have been working on ways to more quickly identify revenue losses from schemes involving permit imprint mail. This effort and a related project seek to combine data culled from a wide range of mailings into a single clearinghouse, to include not just the Permit Imprint System but a host of other major mail systems. Centralizing the data will allow Inspectors to address losses that occur from multiple sources, including short-paid parcels—another growing revenue concern.

Postal Inspectors have established working relationships with BMEU staff across the country, where large quantities of permit imprint mail are received and processed. Their regular interactions ensure that postal employees promptly notify Inspectors when they suspect fraud.

In FY 2010 Postal Inspectors conducted 334 revenue investigations, arrested 68 suspects, and reported 65 convictions. In the course of their investigations Inspectors identified more than $110 million in losses to the Postal Service.

Following are some revenue investigations conducted by Inspectors in FY 2010:

- In February Postal Inspectors arrested the owner of a mailing services business and two former postal employees in Missouri following their indictment for elaborate postage fraud; one employee of the business pled guilty days later. Inspectors found the owner...
devised various schemes: He claimed he affixed pre-cancelled stamps to bulk mailings but instead used permit imprint indicia; his employees obtained signatures and postal “round-date stamps” on forms not included in statements submitted to the Postal Service; and his employees removed pertinent forms from postal employees’ work areas before mail was verified and postage deducted from his company’s account. Estimated losses to the Postal Service exceeded $4 million.

- Postal Inspectors arrested the owner of two Texas mailing companies and five of his employees in June following a seven-count indictment alleging conspiracy, mail fraud, and postage meter fraud. Inspectors found they were using tampered postage meters to affix counterfeit postage to large mailings, resulting in more than $14 million in lost revenue to the Postal Service; they submitted false claims for another $3.9 million worth of unearned refunds. Inspectors initiated their investigation after finding discrepancies between projected revenue and the actual amount of prepaid postage.

- A California man was sentenced in September to two years and six months in prison and three years’ supervised release, and was ordered to pay $270,000 in restitution for defrauding the Postal Service and credit card issuers of as much as $500,000. Inspectors found the man used fraudulent credit cards at automated postal centers (APCs) around the country to make numerous purchases of “Forever” stamps. Although APCs from Florida to Massachusetts to California and states in between had captured photos of the suspect, he concealed his identity by wearing wraparound sunglasses. Inspectors learned he frequently returned to Southern California to purchase stamps and arrested him at the Sun City, CA, Post Office.
As Chief Security Officer for the Postal Service, the Chief Postal Inspector is responsible for the physical protection of all postal personnel, facilities, and assets, as well as the Postal Service’s information security program. The Chief Postal Inspector maintains liaison with other investigative and law enforcement agencies, including the Department of Homeland Security (DHS).

Securing Employees

The Postal Inspection Service initiates background investigations and adjudicates security clearances for postal employees and contractors. Staff at its Security Investigations Service Center (SISC) is tasked with digitizing and archiving security files for criminal cases as well as ongoing investigations documentary evidence.

SISC staff received approximately 45,000 requests for background investigations and security clearances over the past fiscal year. Most requests involved postal contractors, who are required to have some level of security clearance before they can access mail or facilities. SISC staff also provided assistance to Inspectors conducting personnel security reviews for both airline and highway contract route audits.

Personnel Screening

During FY 2010, Postal Inspectors performed follow-up reviews of both highway contract route and contract delivery service drivers to ensure that deficiencies Inspectors identified during their reviews in FY 2009 were resolved. Postal Service policy requires that all such contractors be screened to determine their eligibility as drivers and for access to the mail and facilities. The drivers were checked to confirm they held a current Postal Service security clearance, a valid postal identification badge, and a valid driver’s license. Postal Inspectors worked with district management to correct any noted deficiencies.

Securing Facilities

Postal Inspection Service efforts to secure postal facilities come in many forms, from upgrading and maintaining access controls to reviewing security aspects at postal facilities, where Postal Inspectors recommend improvements and help bring them into existence. Postal Inspection Service oversight for the security of U.S. Mail extends to contractors’ facilities as well.

Facility Security Reviews

New postal facilities are safer for employees, customers, and postal assets because Postal Inspectors, working with staff from the Postal Service’s Facilities office, assess risks to ensure that appropriate and cost-effective safety measures are incorporated into construction plans. This process not only improves security, but also holds down construction costs by anticipating needs and eliminating expensive retrofits.

Besides evaluating construction plans for new or renovated facilities in FY 2010, Postal Inspectors also conducted security reviews at 130 of the most critical existing postal facilities and made recommendations for any needed improvements.

The Security Control Officer (SCO) Program designates a postal facility manager or the manager’s designee as the person responsible for ensuring security at each facility. Postal Inspectors developed online training on facility security to ensure SCOs have the necessary knowledge to secure their offices. Approximately 15,000 SCOs completed the training in FY 2010.
Access-Control Protection for Postal Facilities

The Postal Inspection Service continued its joint project with the Postal Service office of Information Technology to enhance internal security for employees and assets at postal facilities by implementing the Enterprise Physical Access Control System (ePACS).

The system has expanded to almost 200 postal facilities nationwide, which required migrating data from nine access-control databases into a single national database. In a parallel initiative, staff members introduced a nationally standardized employee ID badge, and work began to convert previous versions of employee badges to the new standard.

Retail Security

Postal Inspectors completed an evaluation of the Registered Mail Remittance Program for a specific postal district and then expanded that review to cover a broader area. Staff members charted the flow of postal assets from the Post Office at the point of origin through the postal network to a banking facility. The collected data and results will be used to evaluate any needed changes in future security measures designed to protect postal assets.

Securing Mail Transportation

A major part of the Postal Inspection Service’s commitment to maintaining mail security for postal customers is represented in the protection provided by Postal Inspectors, who must ensure the safety of mail in transit, from its collection to its delivery. Just in the last fiscal year, the Postal Service transported a staggering 1.7 trillion pounds of mail by air to reach postal customers in this country and around the globe.

To this end Inspectors conducted security reviews at 24 airport sites in FY 2010, scrutinizing not only postal facilities that handle mail at airports, but also terminal handler sites and commercial airline facilities. Inspectors visited sites to observe firsthand how mail was transported to and from these facilities and as it moves on airline ramps.

Inspectors’ reviews focused on whether mail was being properly safeguarded while it was handled by suppliers, whether physical security for mail was provided during processing at facilities, and whether contract personnel underwent required background screening. Any opportunities for improvement found by Postal Inspectors were shared with postal managers, and Inspectors conducted follow-up visits to ensure their recommended changes were implemented.

Aviation Security staff of the Postal Inspection Service concentrate on developing and deploying processes that will protect mail in transit in compliance with Title 39 of the Federal Code of Regulations and in agreements with other agencies. Their focus is to establish policies that will mitigate risks posed by mail which could potentially harm postal employees or customers.
Postal Inspectors investigate criminals who misuse U.S. Postal Service money orders—either to launder illicit funds, evade taxes, or avoid federal reporting requirements in violation of the Money Laundering Control Act and the Bank Secrecy Act. Illicit funds may be derived from a variety of unlawful activities, such as illegal drug sales, mail fraud, identify theft, human trafficking or selling counterfeit merchandise, among others.

Postal Inspectors arrested 203 suspects in FY 2010 on charges related to money laundering and reported 170 convictions as the result of their investigations in this and prior periods.

Here are two examples from the past fiscal year:

- Postal Inspectors working with agents from the FBI, ICE, and Federal Reserve Board-OIG determined that a Valencia, CA, woman had defrauded 14 commercial developers of $3.81 million. She took out advance deposits on nonexistent loans from the Federal Reserve and laundered the fraudulent proceeds though multiple bank accounts; Inspectors found she converted most of the money into postal money orders. She was arrested and pled guilty to wire fraud, money laundering, and impersonating a Federal Reserve employee and was sentenced in June 2010 to eight years in federal prison.

- A tip from a window clerk at the Manhattanville, NY, Post Office in March 2008 led Postal Inspectors to investigate suspects who were cashing large numbers of postal money orders. Inspectors tracked about $143,000 worth of the money orders to military post offices in Afghanistan, where the money orders were purchased before being cashed at Post Offices in New York or deposited into suspects’ bank accounts. One suspect in Afghanistan who was receiving $200,000 to $250,000 in gratuities from subcontractors he supervised surrendered to Postal Inspectors after pleading guilty to money laundering. He was sentenced in December to more than three years in prison and ordered to forfeit $200,000.
ASSURING ASSET FORFEITURE>

The U.S. Postal Inspection Service uses asset forfeiture laws and regulations to target criminals’ financial gains from postal-related crime. When Postal Inspectors investigate drug trafficking, identity fraud, and other financial crimes, they often identify money and assets derived from illegal activity that involves the U.S. Postal Service or the U.S. Mail. When appropriate, they use forfeiture laws to seize those assets.

Postal Inspectors seized 990 illegal assets and secured 808 forfeitures in FY 2010; criminals’ forfeiture-related activity in those cases totaled more than $429.6 million. As a result of successful asset forfeiture actions, the Postal Inspection Service shared more than $6.3 million of forfeited funds with other federal, state, and local law enforcement agencies. In most cases forfeited funds are returned to the victims of crime.

For example, in 2005 Postal Inspectors began an investigation of Payment Processing Center (PPC), a third-party firm. Postal Inspectors found that PPC, following the direction of fraudulent telemarketers, was processing unauthorized debits to customers’ bank accounts. The operators mailed bogus fulfillment material to victims, who later filed fraud complaints with the Postal Inspection Service and the Federal Trade Commission.

Inspectors determined that, in 2005 and 2006, PPC had created approximately $140 million in unauthorized debits from fraudulent telemarketers in the United States, Canada, and overseas. PPC processed the debits through accounts in Philadelphia, retained a fee, and remitted the remaining funds to the telemarketers. As a result of Postal Inspectors’ investigation, an injunction was granted and PPC’s assets, including bank accounts, were frozen. In July 2009, a final order of forfeiture was granted for approximately $2.8 million in proceeds from PPC’s activities. The Postal Inspection Service expects to receive $2.2 million in 2011. A separate criminal investigation is being pursued against the fraudulent telemarketers. ■
PROTECTING POSTAL CUSTOMERS
PUBLIC SECURITY

Postal Inspectors respond when criminals try to use the mail to commit crimes against postal customers—from mail theft to mail fraud and even child exploitation. But prevention is often the best way to fight crime. Inspectors use media campaigns, Internet sites, and other venues to teach people how to spot scams before they become victims. For customers who do fall victim to postal crime, agency staff nationwide are trained to assure victims’ rights are protected.
In 2010 the Postal Service delivered more than 177 billion pieces of U.S. Mail to mailboxes, apartment mailbox panels, Post Office boxes, neighborhood delivery units, and countless versions of ingenious, homemade mailboxes crafted to meet federal standards set by the U.S. Postal Service. Every day, more than 584 million pieces of mail—First-Class letters, parcels, magazines, financial documents, business correspondence, Express Mail, Priority Mail, Registered Mail, international mail, and much more—travel across the country. Planes, ships, rail, trucks, automobiles, and human beings move the mailpieces to their destinations, and the Postal Service delivers them to millions of addresses every week.

Postal Inspectors know that criminals may try to steal mail because it can contain many kinds of valuables—not just jewelry or other expensive items, but also personal and financial information contained in credit card applications and other mailings. By deploying the best security available and by taking preventive measures to help protect and educate postal employees and the public about mail theft, Postal Inspectors work hard to thwart the endless number of schemes that mail thieves employ.
In FY 2010, Postal Inspectors arrested 2,775 suspects for mail theft, and 3,031 mail theft suspects were convicted in cases originating in this and prior reporting periods. Following are examples of mail theft cases investigated by Postal Inspectors in the past fiscal year.

- In February nine members of a mail theft ring in Georgia were sentenced to a combined total of more than 55 years in prison and 45 years of supervised release, and were ordered to pay nearly $3.4 million in restitution for bank fraud and aggravated identity theft. Postal Inspectors identified them after tracking complaints from postal customers who failed to receive checks mailed to them. Ring members stole the checks from the mail and negotiated them at retail stores and casinos in Alabama and Mississippi.

- A mail thief in Ft. Worth, TX, was sentenced in February to five years and three months in prison and five years’ supervised release after pleading guilty to bank fraud. Inspectors found he used bank routing and account numbers stolen from business mail to create counterfeit payroll checks. He and his eight co-defendants also used counterfeit IDs to open bank accounts in the Dallas-Ft. Worth area, deposited the counterfeit checks into the accounts, and then withdrew cash. The case involved a host of other criminal offenses, including producing and distributing methamphetamine, counterfeiting U.S. currency, burglarizing homes and cars, and illegally carrying weapons. Inspectors have identified 400 victims and more than $320,000 in losses.

- A Minnesota mail thief who pled guilty to aggravated identity theft was sentenced in June to six years in prison and five years’ supervised release, and was ordered to pay $154,122 in restitution. Postal Inspectors found he stole mail to obtain victims’ personal information and opened bank and credit card accounts in their names; he also diverted mail containing victims’ checks, credit cards, and other financial information to addresses, including vacant houses and Post Office boxes, he controlled. Inspectors identified 250 victims of mail theft among his 400 victims.

- In March 2010 two identity thieves who targeted more than 300 victims were sentenced in federal court in Florida, one to 99 months in prison and the second to 57 months in prison, each with three years’ supervised release. Postal Inspectors found the men, who were ordered to pay restitution of $44,967, opened bank accounts online in victims’ names; fraudulently ordered checks and ATM, debit, and credit cards under the accounts; and filed false changes of address so the checks and cards were mailed to addresses under their control.
Volume Attacks

Volume attacks are a particularly damaging form of mail theft because they can endanger postal employees and customers. These attacks occur when thieves seeking large volumes of mail target postal vehicles, collection and relay boxes, apartment mailbox panels, cluster box units (CBUs), and neighborhood delivery and collection box units (NDCBUs). The Postal Inspection Service devotes significant resources to protecting these assets, and Postal Inspectors work closely with the Postal Service’s Engineering, Collection, and Delivery offices to continually evaluate the need for and deploy new types of security measures for all of them.

The number of volume mail attacks reported in 2010 decreased by 12 percent, falling to 2,251 from the 2,550 reported in 2009. Postal Inspectors aggressively investigated each of these thefts. Here are some examples:

- In January 2010 a confessed drug dealer in Texas was sentenced to 47 months in prison after pleading guilty to possessing stolen mail. He was apprehended by Inspectors after a postal customer witnessed him stealing mail from a neighbor’s curbside delivery box. Inspectors who searched the suspect’s home seized checks, credit cards, and stolen U.S. Mail belonging to more than 50 victims, who suffered more than $90,000 in losses.

- In Boise, ID, a California gang member was sentenced in January to 34 months in prison and three years’ supervised release for possessing stolen mail and unlawful possession of a firearm. Postal Inspectors investigating thefts from some 100 residential and cluster mailboxes apprehended the man with more than 230 pieces of stolen mail, including mail containing checks, debit cards, and blank checks; he was also in possession of firearms stolen in a residential burglary and was driving a stolen car. Another suspect was detained in California pending prosecution.

- Postal Inspectors investigated eight volume mail theft attacks that resulted in $90,000 in victim losses in Camden, NJ, where suspects were breaking windows of postal vehicles to steal mail. Inspectors identified two suspects who were following letter carriers on their routes and stealing government checks from mailboxes and postal vehicles. The thieves used fraudulent IDs in the names of payees on the checks and paid others a portion of the proceeds when they cashed the checks in Camden; Philadelphia, PA; and Raleigh, NC. Inspectors have arrested three suspects since May 2010, and one was convicted in January 2011.

Inspectors in Richmond, VA, educated the public about fake checks to help prevent fraud at financial institutions.
Mail Theft by Contractors

Businesses contracted by the Postal Service to transport the nation’s mail to postal facilities work diligently to do so. These individuals take their responsibilities seriously, just like postal employees. Unfortunately, however, a small percentage of contractors abuse the public’s trust. In FY 2010, Postal Inspectors investigated 74 instances of mail theft by contractors who transport mail, arrested 43 suspects, and reported 61 convictions from cases in this and prior years. Here are two examples:

- Postal Inspectors arrested three suspects in June 2010 for stealing mail from an airport warehouse in Denver, CO. All three were employees of a company subcontracted by an airline that was under contract to transport U.S. Mail. The investigation began in April 2010 when Inspectors learned that mail had been rifled on flights originating in Denver. They identified one suspect when he cashed a gift card stolen from the mail. All three admitted to stealing mail, and their contracts were terminated. They each pled guilty to mail theft: One man was sentenced in December 2010 to a year and nine months in prison, and another was sentenced to a year of probation. Sentencing is pending for the third suspect.

- Inspectors received complaints from postal customers who mailed greeting cards containing cash or gift cards when the rifled cards arrived with the cards or cash missing. Inspectors also learned from security officials of a major company that a large number of mailed DVDs were missing in the same neighborhoods. Inspectors interviewed a Postal Service highway contract route driver, who they arrested in December 2010 after he confessed to the thefts. When Inspectors searched his home they found 225 stolen DVDs, gift cards, letters, and small parcels.
FIGHTING MAIL FRAUD

Dating to 1872, the Mail Fraud Act was the nation’s first consumer protection law, and more than 130 years later it remains a powerful tool to fight mail fraud. As the agency responsible for fighting criminals who misuse the postal system to scam the American public, the Postal Inspection Service enforces the statute to the maximum extent possible against countless illegal schemes seeking to separate postal customers from their money.

Mail fraud cases can be complex, involving intricate dealings designed to confuse investigators as well as victims, and they can be historic. Charles Ponzi’s legendary swindles in the early 20th century—so vast they have given his name (Ponzi schemes) to pyramid-type fraud in general—are constantly being reinterpreted and refined by 21st century criminals bent on investment fraud, telemarketing schemes, and other fraud conducted through the mail, lending credence to the saying, “The more things change, the more they stay the same.”

As the schemes have evolved and their ranges increased globally via the Internet, the Postal Inspection Service has requested assistance from other domestic and international law enforcement entities to leverage resources and maximize expertise in combating them. The Chief Postal Inspector represents the Postal Service on the Attorney General’s Organized Crime Council, which was formed to develop a national unified strategy to combat organized crime. Additionally, the Postal Inspection Service was requested by President Obama to join the Financial Fraud Enforcement Task Force to hold accountable those who helped bring about the last financial crisis, and to prevent another crisis from happening.

In the last fiscal year Postal Inspectors initiated 589 new fraud cases, and Postal Inspection Service analysts prepared more than 76,955 letters and informative postcards in response to mail fraud complaints. Postal Inspectors arrested 1,007 mail fraud suspects and reported 964 convictions as a result of investigations conducted in FY 2010 and prior fiscal years.

Some of the common mail scams investigated by Postal Inspectors include:

- Investment fraud.
- Mortgage fraud.
- Foreign lottery and sweepstakes fraud.
- Fake check scams.
- Mystery shopper and work-at-home scams.

Unraveling Multimillion-Dollar Investment Fraud

A fraudster was sentenced in Minnesota in April 2010 to nearly 10 years in federal prison and three years’ supervised release for running a Ponzi and mail fraud scheme via his purported investment company, Crossfire Trading LLC. Victims mailed checks or wired money to Crossfire’s bank account and were mailed false monthly summaries of their “investments and gains.” The man claimed to be a profitable day trader in futures contracts, earning 36 percent annual returns, but rather than trading investors’ funds, he used their money for his own gain and caused his customers to lose more than $20 million. In addition to his prison sentence, he was ordered to pay $21.8 million in restitution, and he forfeited more than $3.8 million in assets, including a yacht and a John Deere tractor seized by Postal Inspectors when they arrested him in February 2009.
Lottery Scams Damage Thousands

Beginning in 2005, Postal Inspectors identified five men as the operators of a massive foreign lottery scam and fraudulent pension scheme that swindled at least 17,000 mostly elderly postal customers out of more than $17 million. While the names of the offers changed constantly (the Shamrock Agency, New York Super 7, Mutual Medical Insurance Company, and many other names) the results were unanimous—not one postal customer won a thing. One man was extradited from Costa Rica after serving a sentence for murder. He pled guilty to one count of mail fraud and was sentenced to four years and three months in prison and three years’ supervised release.

Inspectors arrested another man in California in May 2007—the same year he was forced to resign from the California State Bar. He pled guilty to mail fraud and was sentenced to two years in prison, a year of home confinement, and three years’ supervised release; he was also ordered to pay a fine of $10,000.

A suspect extradited from Italy was sentenced to two years and two months in prison followed by three years’ supervised release after pleading guilty to one count of mail fraud. The fourth suspect was extradited in 2007 from Amsterdam; he pled guilty to one count each of mail fraud and conspiracy, and was sentenced to a year in prison and two years’ supervised release. Prosecution is pending for the fifth suspect.

Stopping Deceptive Mail

Most sweepstakes are legitimate and appropriate marketing devices, but to protect the integrity of the mail, Postal Inspectors examine questionable promotions and review complaints from postal customers about potentially fraudulent mailings.

Any item sent through the U.S. Mail must comply with the Deceptive Mail Prevention and Enforcement Act, which covers “sweepstakes mailings, skill contests, facsimile checks, and mailings made to resemble government documents.” It grants the Postal Service subpoena power to obtain records and hold administrative hearings to determine the legality of mailings suspected of violating the Act.

The law is specific about what marketers can and cannot do, and it gives the Postal Service the ability to impose civil penalties on violators. Postal Inspectors protect customers by enforcing the Act and submitting requests to the Postal Service’s Judicial Officer for subpoenas or Withholding Mail Orders as needed. Withholding Mail Orders allow Postal Inspectors to stop mail delivery to violators and return that mail—which often contains payments to the fraudsters—to the senders. These two examples represent the kinds of deceptive mail schemes investigated by Postal Inspectors in the last fiscal year:
In Peoria, IL, a Cease and Desist Order was issued against a woman who conducted a bogus gift card scheme via the mail. She promoted a $1,000 gift card as part of an economic stimulus package, requiring a $119 advance-activation fee to get the card. Victims mailed money to a mailbox she rented at a commercial mail receiving agency (CMRA) in Valley Cottage, NY, and the CMRA forwarded the mail to her home in Peoria. Victims who paid the fee never received a gift card. Postal Inspectors arrested the woman, and she pled guilty to mail fraud in June.

In Alexandria, VA, a Cease and Desist Order was issued against two auto shipping companies operating via the Internet. The owner of the businesses instructed customers to mail shipping payments via Express Mail to a CMRA, but Postal Inspectors found he failed to provide the services promised—and even blocked victims’ phone numbers to avoid receiving their complaints. Approximately 275 postal customers lost in excess of $144,000.

With cross-border partnerships, including these following cases:

- A man in Edmonton, Canada, who was extradited to the United States to face wire fraud charges in Arizona was convicted and sentenced to nearly three years in prison and ordered to pay restitution of $53,724 and a $75,000 fine. Postal Inspectors found he had set up multiple Internet sites falsely claiming an affiliation with The University of Alberta and offering for sale a cancer drug known as DCA—which is not approved by the U.S. Food and Drug Administration and cannot be prescribed by a doctor in the United States or Canada. Thirty U.S. cancer victims bought the drug, which was delivered via the U.S. Mail; additional recipients of the bogus drug were identified in Canada, the United Kingdom, Belgium, and the Netherlands. The investigation was conducted with Canadian authorities affiliated with the Alberta Partnership against Cross-Border Fraud.

- Following an investigation with the Alberta Partnership, an Alberta man was found guilty of defrauding 49,000 consumers of close to $4 million in refunds for Canada’s Goods and Services Tax (GST). Postal Inspectors had received a complaint about a Canadian company, International Tax Refund Service (ITRS), which purported to assist people traveling to Canada by processing GST refunds on their behalf through Canada Customs. Visitors sent reimbursement forms and receipts to ITRS via the U.S. Mail for processing through Canadian Customs. To circumvent Canadian law and regulation, ITRS rented a mailbox at a CMRA in the United States and directed Canadian Customs to mail GST refund checks directly to the CMRA, which forwarded the mail to ITRS in Canada. ITRS negotiated the checks, kept “processing fees,” and mailed partial refunds to U.S. residents. Inspectors obtained a Withholding Mail Order for all mail addressed to ITRS to protect other potential victims. The defendant was sentenced in September to five years in prison.

Working with International Partners

The U.S. Postal Inspection Service and Canadian authorities work together to combat mail fraud through six cross-border partnerships known as Project Emptor, the Atlantic Partnership, Project Colt, the Toronto Strategic Partnership, the Vancouver Strategic Alliance, and the Alberta Partnership. The partnerships cover a large territory close to the U.S. border and focus on combating telemarketing and mass-marketing fraud aimed at U.S. and Canadian citizens. Postal Inspectors are formalizing two new cross-border initiatives: another Canadian partnership that will include authorities in the Saskatchewan Province, and a Jamaican partnership to combat fraud targeting U.S. consumers from that country.

In FY 2010, Postal Inspectors conducted approximately 40 international investigations associated with cross-border partnerships, including these following cases:
President Obama established the Financial Fraud Enforcement Task Force in 2009 to aggressively investigate and prosecute significant financial crime. The many federal, state, and local law enforcement entities that comprise the task force were directed to exact just punishment for the perpetrators of these crimes and make every effort to recover the money lost by victims. Operation Broken Trust, a Task Force initiative from FY 2010, encompassed a four-month, nationwide sweep attacking financial fraud.

Operation Broken Trust represents the first national effort to tackle fraud against the investing public. From August through December 2010, it resulted in combined enforcement actions against more than 340 criminal defendants and 189 civil defendants for scams that devastated more than 120,000 citizens, who together lost an estimated $2 billion.

The U.S. Postal Inspection Service announced its Operation Broken Trust results in December 2010: Postal Inspectors’ investigations had identified 31,195 victims of financial schemes, whose victims lost a combined $602.1 million of their hard-earned money—in many cases representing their entire life savings. These cases illustrate Inspectors’ successes in stopping these damaging scams:

- The owner of a purported investment company in Omaha, NE, was sentenced in November 2010 to five years in federal prison and three years’ supervised release for running a Ponzi scheme that drained more than $8.2 million from at least 25 victims. He promised his customers they would see a seven to nine percent annual return on investments from his company. But Postal Inspectors determined that the business he promised would provide those returns was just another failing company he owned, and only the first few people who signed on to his program received any returns on their investments. Instead, he used victims’ money to fund a lavish lifestyle, prop up his many failing businesses, and make monthly payments to previous investors. He relied on the U.S. Mail to distribute fraudulent information to his investors and to receive their money. The judge ordered him to pay $6.8 million in victim restitution.

- A federal court judge in New York handed down a nine-year prison sentence in May 2010 to a man who deceived at least 199 of his fellow church members in a Ponzi scheme that robbed them of a combined $2 million. He began the scam in 2007, offering members of his church and at least four other churches the chance to invest in an electronics company that he vowed would bring returns of 30 to 39 percent. Postal Inspectors located and interviewed the trusting victims who had mailed him their checks. But only early investors received any returns on their funds—and only for a short period of time; all of them received phony stock certificates and bogus investment statements in the mail. He was convicted of mail and wire fraud following a six-day trial, and the judge ordered him to pay $2 million in restitution to victims. An Inspector fluent in Spanish worked to interview the victims, who were Hispanic, and more victims are still being located.
Operation Stolen Dreams is the federal government’s largest-ever mortgage fraud takedown. Launched in March 2010, this multi-agency initiative has led to 485 arrests, more than 330 convictions, and nearly $11 million in seizures. Losses to home buyers and lenders are estimated to exceed $2 billion.

Unlike previous mortgage fraud sweeps, Operation Stolen Dreams seeks justice not only through federal criminal cases, but also in civil enforcement and restitution for victims. As members of President Obama’s Financial Fraud Enforcement Task Force, the U.S. Postal Inspection Service and many other federal, state, and local agencies that joined the initiative have been sharing intelligence and industry data to cooperatively identify illegal mortgage activities nationwide.

Mortgage fraud can take many forms, ensnaring the elderly through straw purchases of properties or targeting immigrant communities that are unfamiliar with mortgage processes. Loan-origination scams, short sales, property flipping, and equity skimming can bankrupt personal lives, bring down property values, and destroy entire communities. Here are examples of investigations undertaken by Postal Inspectors in FY 2010:

- Following more than six hours of deliberation, a jury in St. Paul, MN, convicted a man who had passed himself off as a mortgage broker and credit repair specialist on all counts against him—including six counts of mail fraud. His mortgage fraud and equity-skimming scheme robbed approximately $400,000 from homeowners who believed they were “only refinancing” their homes, not having their homes sold without their knowledge. Postal Inspectors found he targeted more than 35 homeowners who were either in foreclosure or behind on their mortgage payments. He intercepted their equity checks, deposited them into his own accounts and, in some cases, used physical intimidation to force vulnerable homeowners to endorse their checks over to him. During sentencing, the district court judge stated that society needed to be protected from this “unique danger,” a man “without conscience.” In an upward departure to guidelines, the man was sentenced in April 2010 to 22 years in federal prison.

- A Georgia man still under supervised release for prior mail fraud, bank fraud, money laundering and other convictions was sentenced in April 2010 to 16 years and two months in federal prison and five years’ supervised release for mortgage fraud. His probation officer told Postal Inspectors he received a tip that the man had legally changed his name and was again running various scams. Inspectors found he had defrauded dozens of banks and other lenders by mailing fraudulent documents to obtain mortgage loans, vehicle loans, lines of credit, and credit card accounts. Using several aliases, he filed bankruptcy petitions and used straw borrowers and others to facilitate his schemes. He was convicted of conspiracy to commit mail fraud and was ordered to pay $2.2 million in restitution.
HALTING CHILD EXPLOITATION VIA THE MAIL>

For more than a century, Postal Inspectors have investigated the sexual exploitation of children when it involves the U.S. Mail. The Postal Inspection Service was the first federal law enforcement agency to aggressively identify, target, and arrest those who produce and traffic in child pornography.

Postal Inspectors arrested 115 suspects and identified 25 child molesters in FY 2010 as part of the Postal Inspection Service’s continuing efforts to bring to justice those who unlawfully use the mail to traffic in child pornography or otherwise sexually exploit children. Most significantly, during their investigations Inspectors identified and were able to rescue 54 children from incidents of sexual abuse and exploitation.

Because nearly all cases of child exploitation investigated by Postal Inspectors involve the Internet as well as the mail, the Postal Inspection Service has become an integral partner in Project Safe Childhood, a Department of Justice (DOJ) initiative that combines a wide array of resources from federal, state, and local law enforcement agencies to protect children from sexual exploitation and abuse by online predators. A number of Inspectors’ investigations from the past year were conducted with Project Safe Childhood partners.

In FY 2010, Postal Inspectors initiated 118 new investigations involving the sexual exploitation of children. The investigations included high-impact casework that emphasized identifying and dismantling major commercial distribution enterprises that relied on the mail and the Internet to conduct illegal activities. Postal Inspectors worked in close cooperation with trial attorneys of the DOJ Child Exploitation and Obscenity Section, where a Postal Inspector is assigned full time on all mail-related cases of national and international significance.

A joint press conference held by the U.S. Postal Inspection Service, the U.S. Postal Service, and others in May 2010 commemorated the 25th anniversary of the “Have You Seen Me?” program that helps locate missing children. A mailer delivered to more than 44 million homes was customized for six regions in the United States and featured 25 missing children specific to those areas. At the press conference former Postmaster General Jack Potter and former Chief Postal Inspector William Gilligan recognized a San Francisco Division Postal Inspector and the Postmaster of Naco, AZ, for their extraordinary efforts to locate and identify multiple victims of child molestation.

Here are examples of investigations conducted by Postal Inspectors during FY 2010:

▪ After entering a guilty plea, a Danville, IL, man was sentenced to 40 years in prison for producing, advertising, receiving, and possessing child pornography. He was identified after Postal Inspectors learned he had purchased and received child pornography from a former commercial mail-order child pornography enterprise. Inspectors executed a federal search warrant at his home and seized evidence that led them to identify a second offender, as well as numerous minor-age male victims nationwide whose images were being traded extensively on the Internet.

▪ An Atlanta, GA, man was sentenced to 15 years in federal prison and a lifetime of supervised release after he was found guilty of using the mail to distribute child pornography. He had been released from prison in 2009 after serving 15 years for molesting his five-year-old daughter; after his release, Postal Inspectors found he mailed child pornography to his former cellmate, who was in the Georgia State Prison.

▪ A retired police officer in Hale, MI, was sentenced to five years in federal prison and a lifetime of supervised release after Postal Inspectors arrested him for the attempted receipt of child pornography via the U.S. Mail. The former officer was a customer of a company investigated by the Postal Inspection Service for distributing child pornography by mail. The man estimated he had molested eight to 11 boys over a 30-year period, some while he was still a police officer, and some quite recently. Michigan State Police are investigating multiple sexual assaults against the minor boys.

AFFORDING PROTECTION TO CRIME VICTIMS>

The rights of crime victims and witnesses have expanded progressively since 1982, when Congress passed the Victim Witness Protection Act. Subsequent legislation—most recently, the Crime Victim Rights Act, adopted in 2004 and amended in 2008—continues to strengthen their protections.

The Postal Inspection Service is committed to working with the Department of Justice (DOJ) and the law enforcement community to support the Attorney General’s Guidelines for Victims and Witnesses. The Postal Inspection Service’s responsibility is to identify potential victims related to its criminal investigations, provide them with timely notification of their rights, and inform them of the services available to assist them.

Postal customers who are victimized by a crime, or witness one, value and remember the personal attention they receive from the Postal Inspection Service. Staff members regularly apprise crime victims of their cases’ status in the judicial process, both fulfilling legal requirements and providing emotional support. Going beyond legal mandates, trained agency staff regularly call and stay in touch with victims to fulfill a host of other needs.

Being a victim of a crime is nothing to be ashamed of... and we can help you recover from it.
Victim Service Outreach

The Postal Inspection Service continues to enhance its victim outreach program, training its personnel as experts in services and resources for victims of crime. This chart reflects the types of service referrals and assistance provided to victims over the past year:

<table>
<thead>
<tr>
<th>Victim Outreach</th>
<th>FY 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifications</td>
<td>72,559</td>
</tr>
<tr>
<td>Information and Referrals</td>
<td>2,677</td>
</tr>
<tr>
<td>Criminal Justice Support</td>
<td>2,046</td>
</tr>
<tr>
<td>Identity Theft Assistance</td>
<td>667</td>
</tr>
<tr>
<td>Senior Assistance</td>
<td>214</td>
</tr>
<tr>
<td>Victim Advocacy</td>
<td>2,502</td>
</tr>
</tbody>
</table>

The Postal Inspection Service is only the second federal law enforcement agency to gain direct access to DOJ’s Victim Notification System. This level of access is necessary because so many Postal Inspection Service investigations, especially those involving mail fraud and mail theft, affect large numbers of victims. DOJ and Postal Inspection Service staffs continue to combine their skills to expand and improve the program, with increasingly successful results. In FY 2010, general analysts mailed victims more than 72,559 notifications via the Victim Notification System.

Know Your Rights

Publication 308, Know Your Rights: A Guide for Victims & Witnesses of Federal Crimes, is key to the Postal Inspection Service’s Victim and Witness Assistance Program. Available in English and Spanish, the guide is used to notify victims and witnesses of their rights and the services available. When the Postal Inspection Service is the lead agency in a crime investigation, staff members provide potential victims with the brochure, which explains their rights related to the investigatory process, including notifications of arrests and other case activity. It offers advice on what to do if they are threatened or harassed and directs them to services that can help them recover from the physical and emotional effects of a crime.
National Crime Victims’ Rights Week 2010

The Postal Inspection Service teamed with DOJ and the National Center for Victims of Crime to showcase National Crime Victims’ Rights Week in April 2010. This year’s theme, “Crime Victims’ Rights: Fairness. Dignity. Respect,” recalls the ideals that inspired the victims’ rights movement and the laws, services, and awareness the Postal Service seeks to promote. These basic human rights, particularly crucial in times of crisis, resonate with victims, service providers, law enforcement, and all the visionaries who help make these ideals a reality every day. Posters and informational literature were distributed to 12,500 Post Offices and more than 7 million customers who visited the facilities in April.

Victim-Witness Assistance

These are examples of assistance provided in FY 2010 to crime victims:

- The owner of Innovative Investment Advisors, Inc. in Herndon, VA, operated a “Bernie Madoff-type” investment scam, defrauding friends, relatives, and clients who trusted him completely. Inspectors revealed he had mailed clients false statements about their investments, failed to set up their accounts, used their funds to trade stock index options, and lost large sums of money; many elderly victims will never be able to recover their funds. An Inspector and Victim Specialist located victims and provided them with counseling and financial referrals. One victim was so distraught by the deceit of his trusted “friend” that he became suicidal—until several calls from the Victim Specialist and a referral to a Suicide Hotline provided help. In July 2010, the scammer was sentenced to more than 12 years in prison and three years’ supervised release, and was ordered to pay $6.9 million in restitution to his victims.

- A postal manager contacted local police and Inspectors in May to report that the Whiteside, TN, Post Office had been robbed at gunpoint by a man who had taken her hostage. Postal Inspectors and a Victim Specialist responded to the scene and assisted the employee, providing emotional support, referring her for Employee Assistance Program counseling, arranging to replace her cell phone stolen in the robbery, and getting her car locks re-keyed, as the suspect had taken her keys. Inspectors developed a suspect who had burglarized and robbed other Post Offices in the area and had been released from prison five months earlier. In September the man was indicted on federal charges after Inspectors arrested him in Georgia. The Victim Specialist and Inspector stayed in touch with the victim throughout the investigation, providing general support and keeping her apprised of her rights and possible compensation.
EDUCATING POSTAL CUSTOMERS

Consumer education is another potent tool used by the Postal Inspection Service to alert postal customers about fraudulent schemes and ways to avoid becoming victimized. Postal Inspectors across the country serve as public information officers (PIOs), trained to proactively communicate with both the media and members of the public. PIOs are also considered “the voice of the Postal Inspection Service”—representing the agency during times of crisis. They provide prompt and accurate messaging for news organizations and members of Congress, but also help protect postal customers by organizing community events at local venues to educate the public about mail-related crime and inform them of current fraud schemes.

Another method the Postal Inspection Service uses to educate consumers and steer them away from fraudulent schemes is through its partnership with the Federal Trade Commission (FTC) during National Consumer Protection Week (NCPW). NCPW is an annual campaign designed to draw attention to issues and ideas that help customers become smarter consumers of products, materials, and services and to improve their knowledge about combating fraud. Each year during NCPW, the Postal Inspection Service works to educate consumers, in cooperation with the Postal Service’s Office of Consumer Affairs; other federal, state, and local consumer protection agencies; consumer organizations; and relevant industry groups.

For this year’s NCPW the Postal Inspection Service undertook an effort to reach the entire mailing public. In a brochure that was mailed to nearly every home in America, Postal Inspectors provided information to help postal customers recognize the warning signs of fraud. Inspectors know that when citizens understand how fraud schemes work, they can protect themselves from becoming victims. This nationwide consumer initiative was made possible by funds collected from criminals convicted of fraudulent schemes.

Fraudsters say:

“An educated consumer is our worst customer.”
Delivering Public Service

The Postal Inspection Service posts fraud alerts, wanted and reward posters, and consumer-fraud information on its Web site, postalinspectors.uspis.gov. Postal customers can report suspected mail theft, identity theft, mailbox vandalism, and mail fraud online at the site or by calling 877-876-2455, available 24 hours a day.

Also offered on the Web site are publications that explain various types of mail-related crime and provide information to help consumers avoid being victimized. In the past year the Postal Inspection Service updated one of its consumer-awareness brochures, Postal Inspection Service Guide to Preventing Mail Fraud (Publication 300-A), to add reshipping schemes as one of the latest “frauds to be aware of.” Reshipping schemes are typically conducted by criminals in Eastern European and West African countries, and involve bogus job offers, fraudulent credit card orders, and the reshipping of illegally obtained products. Criminals use stolen credit cards to buy high-dollar items on the Internet, then have the items shipped to U.S. addresses of “reshippers”—who may be unaware they are handling stolen goods. The reshippers are directed to mail the stolen items overseas. Victimized businesses include Amazon, eBay, and other Internet auction sites.

When it comes to reshipping scams, U.S. Postal Inspectors warn all postal customers:

▪ Don’t give out personal information to a person or company you don’t know.

▪ Be suspicious of any offer that doesn’t pay a regular salary or involves working for an overseas company.

▪ Before you accept a job, check the company with the FTC, Better Business Bureau, or state Attorney General. ■
PROTECTING > THE FUTURE
POSTAL SECURITY

In FY 2010 the Postal Inspection Service focused on maintaining public confidence in the mail, including global security for U.S. Mail. The Global Security and Investigations Division, Cyber Intelligence Division, and National Preparedness staff are essential to meeting agency goals.

Postal Inspectors proactively address crime affecting the Postal Service and its customers by working with domestic and foreign law enforcement and intelligence agencies. Inspectors and other employees undergo thorough training to prepare for emergency responses to ensure readiness for all hazards.
WORKING GLOBALLY>

Rapid technological advances, a rise in global markets, and a relentless worldwide drive for growth have combined to make the world more interconnected. The U.S. Postal Service has accordingly scaled up its international business ventures to meet the demands of this new global environment.

For the Postal Service, the increase in global trade has brought with it opportunities as well as challenges in terms of operations and security. A robust international postal security program is essential to safeguard U.S. postal operations, which generate almost half of the world’s mail. The Postal Inspection Service’s Global Security and Investigations Group coordinates with the Postal Service’s Global Business Operations offices and partners with foreign law enforcement stakeholders to offer unparalleled security coverage to help protect U.S. Mail worldwide.

Postal Inspectors are charged with protecting the Postal Service’s international and military mail assets and operations through worldwide investigations as well as liaison with designated foreign operators, security personnel, and other law enforcement agencies. In addition, Postal Inspectors engage in security consulting missions through the Postal Security Group (PSG) of the Universal Postal Union (UPU) and the Postal Union of the Americas, Spain, and Portugal (PUASP); and other restricted unions, international postal groups, and stakeholders.

Inspectors are domiciled at the Postal Service’s five International Service Centers (ISCs) in Miami, San Francisco, Los Angeles, Chicago, and New York, where mail arrives from other countries. Inspectors’ global investigations resolve significant security issues both in the United States and abroad. Below are some examples of investigations conducted by Inspectors during FY 2010.
Inspectors at the New York ISC investigated allegations of mail theft after receiving complaints about rifled inbound mail on flights originating in Europe and various postal military offices. Covert operations identified several suspects, and in July, Inspectors interviewed two airline contract employees at JFK Airport. One suspect provided a sworn statement admitting he had been stealing mail since November 2009; the other suspect denied involvement in the thefts even though Inspectors observed him stealing mail and acting as a lookout. Criminal charges were filed against both men.

Inspectors in Chicago investigated mail theft allegations after several foreign postal operators reported rifled mail and missing contents from Express and Priority Mail parcels going to Ukraine and Russia. They arrested an airline contractor in August after observing him steal an iPad from the mail while preparing an international mail dispatch. During an interview with Inspectors he provided a sworn statement admitting he had stolen laptops, cameras, and clothing from the mail, and voluntarily turned over stolen property still in his possession. After Inspectors notified his managers, the suspect and three other collusive employees were terminated from their jobs. Criminal charges were filed.

In August Postal Inspectors at the Miami ISC along with agents from the U.S. Secret Service, Immigration and Customs Enforcement (ICE), and Customs and Border Protection seized approximately $1.9 million worth of counterfeit financial instruments seized from two parcels arriving from the Republic of Benin in West Africa. The packages contained 754 counterfeit postal money orders worth nearly $736,000, in addition to American Express Traveler’s Cheques and counterfeit bank checks.

United States National Central Bureau of Interpol

The U.S. National Central Bureau serves as the national point of contact for Interpol matters and coordinates international investigative assistance between Interpol’s 188 member countries and the more than 18,000 federal, state, local, and tribal law enforcement agencies in the United States. The bureau is co-managed by the Department of Justice and Department of Homeland Security, and acts effectively as a task force to support the entire American law enforcement community. It provides access to investigative resources and to police authorities worldwide. These resources include a secure communications network and databases containing information supplied by member countries on wanted persons, stolen and lost travel documents, stolen vehicles, and other law enforcement data.

In FY 2010, Postal Inspectors assigned to the National Central Bureau assisted Inspectors across the country with more than 153 investigative requests with an international nexus. Examples of assistance include obtaining address information for overseas fraud victims; researching criminal histories, photos, and fingerprints of subjects; and issuing notices and diffusions for wanted fugitives. Nine “Red Notices” (which allow a warrant to be circulated worldwide, and request that the suspect be arrested with a view to extradition) were issued for wanted fugitives, and two fugitives were extradited to the United States. Postal Inspectors at the National Central Bureau also assisted field Inspectors in gaining admission for three parolees to the United States through an ICE parole process for witnesses or subjects who do not meet the criteria for entry to this country.
International Liaison

Inspectors at the Miami ISC coordinated a postal security review in La Paz, Bolivia, on behalf of the Postal Service’s office of Global Business Operations. The review was in response to a request from the director general of the Bolivian Post to resume previously suspended parcel service from the United States. Inspectors examining the international receipt of parcels by Empresa de Correos de Bolivia (ECOBOL)—the designated postal operator in Bolivia—determined that security safeguards protecting inbound U.S. Mail had not been improved as previously requested by the Postal Inspection Service, and issues of inadequate airlift between the countries remained. Based on these security shortfalls, the Postal Service determined it would continue to suspend international parcel service to Bolivia.

Haiti Postal Security Mission

On January 12, 2010, a magnitude 7.0 earthquake struck Haiti, with its epicenter 10 miles southwest of the capital city of Port au Prince, and numerous significant aftershocks following the initial tremor. Catastrophic damage, including significant destruction to Haiti Post’s infrastructure, resulted in cessation of mail service in Haiti. A team of Postal Inspectors traveled to Haiti to establish communications and coordinate relief efforts with Haiti Post, along with Postal Service, UPU, and PUASP officials. Inspectors assessed mail conditions, assisted in establishing a secure temporary delivery system, and ensured proper standards for delivering and deploying equipment donations from the Postal Service, UPU, and other stakeholders worldwide. Relief work in Port-au-Prince (and in the UPU-designated mail-staging area of Santo Domingo, Dominican Republic) formed the basis for all additional assistance provided by the UPU and others in the postal sector.
Cuban Mail Service

Postal Inspectors continued to work with staff from the Postal Service’s office of International Postal Affairs and the Department of State to develop and implement security guidelines for establishing direct mail service to Cuba. Inspectors traveled to Cuba as part of a Department of State-led U.S. delegation putting forth security proposals and observing mail-handling operations in the island country. Inspectors also prepared security guidelines and recommendations for the Postal Service, Department of State, and Correos de Cuba, Cuba’s postal service.

International Security Training

As chairman of the UPU’s Postal Security Group (PSG), the Chief Postal Inspector continued his leadership role in ensuring the security of the international mail network. Part of this commitment involves the delivery of security training for employees of foreign postal operators and security stakeholders in support of the PSG.

Postal Inspectors offered training for various countries on methods of improving the security of the international mail network and protecting U.S. Mail as it transits international borders. In August Inspectors led an initiative in Montevideo, Uruguay, on Security Certification and Dangerous Goods in the Mail for PUASP member countries. Also in 2010, Postal Inspectors worked with postal officials from ECOBOL and the U.S. Embassy in Bolivia to provide training to address that country’s problem with letter bombs.

Inspectors also launched a Security Certification project that will be piloted in the PUASP region before being offered to other UPU member countries. The project introduces security training requirements, establishes a security department that reports directly to the country’s highest authorities, requires periodic self-assessments to determine quality of service and security in mail operations, and mandates agreements for external compliance reviews.

Foiling Reshipping Scams

The Postal Service can suffer significant losses as well as damage to its brand integrity when criminal schemes target postal products or services. Criminals who conduct reshipping fraud recruit U.S. citizens by advertising on popular career Web sites, such as monster.com and craigslist.com, and employing classified ads to lure people to “make money while working from home.” Using stolen credit card numbers, the scammers purchase computers, electronics, clothing, and other items that can easily be resold and mail them to recruits for reshipping to other countries. The criminals often provide their reshippers counterfeit “postage-paid” mailing labels.

Statistics collected by Inspectors show that 91 percent of the parcels in reshipping schemes go to Russia, Nigeria, Ghana, Ukraine, and Kazakhstan. Criminals involved in these scams may try to exploit the Postal Service’s Click-N-Ship program to fraudulently obtain and use postage to mail their stolen goods to these counties. To counter the schemes, Postal Inspectors continued a Click-N-Ship initiative started in 2008 by interdicting mail at each of the five ISCs, seeking parcels bearing fraudulent postage-paid shipping labels.

The methodology used by Inspectors in the FY 2010 Click-N-Ship initiative followed a successful pilot program from 2008. The sustained goal is to remove from the mailstream suspect international outbound Express Mail parcels bearing counterfeit postage, particularly Click-N-Ship postage purchased with stolen credit cards or fraudulently reproduced without payment. Postal Inspectors in FY 2010 who interdicted mail at the five ISCs returned 1,794 parcels bearing postage valued at approximately $254,000 and purchased with stolen credit cards or counterfeited.
Foreign Lottery Scams

Postal Inspectors in Miami submitted 125 Determinations of Nonmailability for the destruction of more than 6,000 pieces of inbound lottery mail from Canada containing $24.6 million worth of counterfeit checks. Inspectors seized another 7,000 pieces of mail destined for Panama and containing about $25 per envelope, sent by postal customers to claim their alleged “winnings” for bogus lottery and sweepstakes drawings. Inspectors seized and returned all outbound mail to the unsuspecting victims.

Combating Counterfeits

Postal Inspectors continued their partnership with agents from U.S. Customs and Border Protection in FY 2010 to identify transnational criminal rings responsible for counterfeiting postal money orders, stamps, and meter stamps. Inspectors’ interdictions of counterfeit documents from West Africa resulted in the seizure of approximately 27,000 counterfeit money orders valued at $26 million.
PATROLLING CYBERSPACE>

The U.S. Postal Inspection Service takes an aggressive approach to investigating cybercrime affecting the U.S. Postal Service and its customers, and develops solutions to mitigate these threats by:

- Targeting high-value crime affecting the Postal Service and postal customers.
- Building and maintaining relationships with foreign and domestic law enforcement and intelligence agencies, businesses, and academic institutions.
- Providing timely, accurate reporting of cybercrime risks to Postal Service business ventures.
- Mitigating risks to new postal products and business planning.

With about 500,000 career employees and approximately 32,000 locations, the U.S. Postal Service not only is one of the largest businesses in the United States, but also owns one of the world’s largest information technology infrastructures. Its international operations continue to expand.

All Postal Service operations—including mail processing, accounting, payment systems, and payment disbursements—rely on its IT infrastructure. Further, postal customers use numerous Web-based products, such as Click-N-Ship, Change of Address and Hold for Pickup services, and Post Office Box payments. Just like other companies and government agencies around the globe, the Postal Service faces thousands of network attacks daily by criminals seeking access to its computers in a bid to create havoc or steal assets.

Securing the Postal Infrastructure

Every day, more than a million people visit usps.com to track packages, buy stamps, ship parcels, look up a ZIP Code, and conduct countless other types of business. To provide its customers with a premium online experience, the Postal Service continually explores new technologies to enhance its portals with increased functionality, services, and products. Much of this work is transparent to the average user, but cyber criminals pay close attention to every new development; for them, the Internet poses endless possibilities for fraud.

To combat Internet crime, the Postal Service turns to Postal Inspectors with special expertise and advanced training in deterring, detecting, and investigating cyber threats. Inspectors work directly with software programmers, product developers, and information technology experts tasked with expanding online postal services. Their input is invaluable, ensuring that Postal Service revenue is protected, customer information is kept private and secure, and the network infrastructure remains stable and secure against criminal exploitation.

Researching Cyber Threats

In FY 2010 the Postal Inspection Service continued to partner with the National Cyber Forensics and Training Alliance, a non-profit organization that works with law enforcement agencies, private industry, and academia to research cyber attacks.

Postal Inspectors in this group use a “malware” analysis program to secure the Postal Service’s information technology infrastructure by identifying emerging cyber threats and providing timely analysis to postal executives and the Postal Service’s Computer Incident Response Team. Inspectors also perform “reverse engineering” of malicious code that threatens or infiltrates postal systems.
Arming Against Cyber Attacks

The U.S. Postal Inspection Service entered into a working agreement with the Computer Emergency Response Team (CERT) Certification Center, located on the campus of Carnegie Mellon University in Pittsburgh, PA. Postal Inspectors on the CERT team strive to address existing and potential cyber threats affecting the Postal Service, notify system administrators and other critical entities of problems, and coordinate with vendors and incident-response teams to address risks to the Postal Service’s technology infrastructure.

These are some of the projects completed by the Postal Inspection Service team assigned to CERT in the past year:

- Postal Inspectors at CERT were alerted to more than 1,100 e-mails containing fraudulent solicitations purportedly sent by the Chief Postal Inspector. To shut down the questionable accounts, Inspectors coordinated agreements with businesses—including Microsoft, Google, Yahoo!, and America Online—that (unknowingly) hosted the fraudulent e-mails.

- Clustered-Computing Analysis Platform (C-CAP) is a state-of-the-art forensics analysis platform for examining and analyzing digital evidence. Postal Inspectors are using this tool to shorten the time needed to conduct large-scale cyber investigations.

- The Postal Inspection Service supports the Postal Service by evaluating key infrastructure security mechanisms against best practices defined by the Resiliency Management Model (RMM). Inspectors are making security and sustainability recommendations to help improve the Postal Service’s ability to maintain critical systems necessary to delivering the organization’s products and services.

- More than 100 Postal Inspectors and postal employees have taken advantage of Virtual Training Environment (VTE) published studies, handbooks, live demonstrations, and recorded lectures on a wide array of cyber-based topics available via the CERT VTE portal.

Additionally, Inspectors are participating in the Merchant Risk Council’s monthly Law Enforcement Working Group, developing a Cyber Intelligence Investigative Resource Guide, and conducting a CERT-managed review of the Postal Inspection Service’s Intranet.

Securing Online Click-N-Ship Revenue

The Postal Inspection Service works with several Postal Service offices to deter fraud on the usps.com site. The Online Fraud Detection Application and more than 130 “fraud rules” flag suspected illegal transactions. In FY 2010 Postal Inspectors tallied these successes:

- Blocked 40,208 online Click-N-Ship accounts.
- Prevented nearly $9.9 million worth of fraudulent online transactions.
- Identified 48,208 credit cards that were used fraudulently.
- Blocked 22,873 IP addresses associated with Click-N-Ship transactions.
RESPONDING EFFECTIVELY

National Preparedness

The Postal Inspection Service works hard to protect postal employees, customers, and operations by instituting national preparedness capabilities that anticipate evolving threats to Postal Service interests. To achieve this vision, its National Preparedness Group has set a goal of maintaining a high state of preparedness through comprehensive and coordinated planning, integration, and support.

Homeland Security Coordinators work directly with Postal Inspectors to ensure readiness in addressing “all-hazards” events—incidents with urgent public health consequences. They respond to these events nationwide by implementing risk-mitigation plans and procedures, as well as incident response and recovery operations.

Deploying Emergency Resources

The Postal Inspection Service implemented, managed, and refined emergency resources over the past fiscal year, including its contracts for Emergency Preparedness Response and Recovery Services, the Large Capacity Power Generator Program, Critical Reserve Stockpile, National Alert System, and Geo-Spatial Information Systems—all designed to protect postal employees, assets, and infrastructure. The programs reinforce the agency’s adherence to the National Response Framework, which guides all national preparedness activities for federal, state, and local entities.

Conducting Emergency Response Tests, Training & National Exercises

The Postal Inspection Service uses Incident Management & Recovery Services Programs, such as the Large Capacity Generator Program and the Critical Reserve Stockpile, to maintain postal operations during emergencies, provide needed resources, and reduce interruptions to mail operations. Supporting speedy and efficient recovery efforts supports trusted relationships between the Postal Service, its employees, and its customers by meeting performance standards for mail delivery.

Maintaining postal operations during emergencies is further enhanced by Integrated Emergency Management Plans (IEMP), which focus on actions taken to prepare for, respond to, recover from, and mitigate all-hazards emergencies or incidents. In accordance with the National Response Framework and the National Incident Management System, IEMP provides a comprehensive framework for managing emergencies. It also delineates Emergency Management Team roles and responsibilities to enhance communication, coordination, and recovery.

The Postal Inspection Service continued to participate in local and national emergency response programs in FY 2010, including the Federal Emergency Management Agency’s Homeland Security Exercise and Evaluation Program. This program sets a national standard for all exercises to help agencies achieve objective assessments of their capabilities, ensuring that strengths and areas for improvement are identified, corrected if necessary, and shared.

The Postal Inspection Service participates in both full-scale and Tabletop Exercises that help evaluate its Emergency Management Planning and Response capabilities. In FY 2010, the Postal Inspection Service conducted 24 Tabletop Exercises at postal facilities nationwide to evaluate response capabilities resulting from a Biohazard Detection Systems (BDS) Response, Pandemic Influenza, and Bomb Threat scenarios. The Tabletop Exercises were augmented by 36 full-scale exercises and drills that ensure the Postal Inspection Service can quickly respond to the needs of the Postal Service in any emergency.
Natural and Manmade Disasters

The Postal Inspection Service actively responds to all emergencies related to natural and manmade disasters that can impact postal operations, such as hurricanes, floods, and fire. Staff members coordinate the deployment of emergency equipment and supplies, and assist with damage assessments and recovery, including hazardous and toxic-material removal. Postal Inspectors strive to educate employees and customers through public-awareness programs about non-mailable and restricted items to promote the continued safety of the mail.

Postal Inspectors continued to conduct risk-assessment reviews at postal facilities nationwide throughout FY 2010. The reviews emphasized specific areas and were tailored to meet risks inherent to each geographical region. The staff evaluates compliance with requirements for building and vehicle security, accountable mail handling, and the local enforcement of employee ID requirements.

Postal Inspectors and Homeland Security Coordinators participated in national responses to these incidents, which impacted postal employees and operations in FY 2010:

- Wildfires, Southern California, October 2009.
- Flooding and storms, Northern California, October 2009.
- Hurricane Ida, Mobile, AL, November 2009.
- Earthquake, Eureka, CA, January 2010.
- Flooding and landslides, Southern California, January 2010.
PROTECTING INVESTIGATIVE ASSETS
TECHNICAL SECURITY

Supporting the often intricate and sensitive intelligence required to investigate criminal acts involving the mail, misuse of the postal system, and attacks against postal employees or customers are four Postal Inspection Service groups: the Career Development Unit—which operates the National Training Academy, the National Forensic Laboratory, the Digital Evidence Unit, and the National Law Enforcement Communications Center.
In FY 2010, forensic examinations identified 479 suspects in criminal cases, matching 90 of them to subjects in the Automated Fingerprint Identification System (AFIS). On 17 occasions, Laboratory personnel gave expert testimony related to the examination and analysis of evidence obtained from Inspectors’ cases.

Laboratory Analysts completed more than 1,700 requests from Postal Inspectors; they examined about 45,000 exhibits, including audio, video, and physical evidence such as documents, fingerprints, and controlled substances. They assisted in cases involving threats against a Postal Inspector and the assault of a postal employee by identifying suspects through handwriting and fingerprint samples and through expert testimony on the analysis and association of paint samples.
Forensic Document Examiners scrutinized about 20 cases involving 4,500 exhibits of such items as stamp coils, stamp books, and stamped mail, finding more than 33,000 counterfeit stamps. They also examined altered postal money orders to determine the method of alteration and to identify subjects through fingerprint analysis.

Experts from the Physical Evidence Section helped solve a Post Office robbery by matching toolmarks taken from various surfaces to tools recovered from suspects, and by matching one suspect’s shoe with a dust print from the loading dock of the Post Office.

Forensic Latent Print Analysts and Forensic Chemists expedited their analyses of fingerprint and chemical evidence on numerous mailpieces containing controlled substances.

In January 2010, staff at the National Forensic Laboratory was successful in gaining accreditation from the Crime Laboratory Accreditation Program of the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB).

This voluntary program allows crime laboratories to demonstrate that their management, operations, personnel, procedures, equipment, physical plant, security, and health and safety procedures meet established standards. Gaining accreditation was the product of nearly two years of dedicated work on the part of the forensic staff. The accreditation process encompassed documenting more than 200 procedures, writing manuals and forms to cover all forensic operations, and preparing more than 350 records to support program compliance.
The Postal Inspection Service operates a National Training Academy at the William F. Bolger Center for Leadership Development in Potomac, MD, to train Postal Inspectors and Postal Police Officers (PPOs) in skills appropriate to their duties. Staff at the academy analyze, develop, implement, and deliver Basic Training for candidate Postal Inspectors and for candidate Postal Police Officers, as well as In-Service Training for both groups.

The Postal Inspection Service has gained accreditation from the Federal Law Enforcement Training Accreditation (FLETA) for its National Training Academy, for its program of Basic Training for Inspectors, and for Basic Training for PPOs. FLETA mandates that programs be reaccredited every three years, requiring academy staff to continually work to maintain accreditation.

Postal Inspector candidates undergo 12 weeks of mostly scenario-based training on investigative techniques, defensive tactics, firearms, legal instruction, search and seizure tactics, arrest techniques, court procedures, Postal Service operations, and in-depth examinations of the federal laws for which the Postal Inspection Service has jurisdiction. The training focuses on problem-solving, critical thinking, and cognitive skills. All candidate Inspectors must successfully complete academic, firearms, and practical exercises to graduate from the program. Over the past fiscal year, academy staff conducted one Basic Inspector Training session, graduating 22 new Postal Inspectors.

Academy instructors also conducted two eight-week sessions of Postal Police Officer Basic Training, and 38 PPOs graduated. PPO candidates receive training on firearms, defensive tactics, and officer survival. Also covered are arrest laws, CPR procedures, bloodborne pathogen handling, critical-incident responses, and interviews of witnesses and victims of crime.

Training for professional, technical, and administrative personnel of the Postal Inspection Service is offered as needed. In the past fiscal year staff conducted 50 sessions of 28 in-service training courses for 646 professional, technical, and support personnel of the Postal Inspection Service. In July 2010, FLETA’s Office of Accreditation conducted an assessment of the Postal Inspection Service Facilitator Training Program, which is required for all instructors and subject-matter experts who develop or revise courses. The program is on track to gain reaccreditation in April 2011.
Here are examples of work performed by the Digital Evidence Unit during FY 2010:

- Forensic Computer Analysts seized 114 computers and captured data from several servers during searches conducted over two days at seven locations in Phoenix, AZ, related to a mail fraud case. Servers at the suspect company’s headquarters location proved extra challenging to analysts since adjoining businesses, unrelated to the criminal investigation, had shared access. Analysts overcame this challenge and successfully copied the needed data.

- What started as a request for a routine analysis of a smartphone seized by Inspectors resulted in a trove of useful evidence for a Flint, MI, investigation. Forensic Computer Analysts were able to recover victim identifiers such as names, addresses, Social Security numbers, dates of birth, user names, passwords, and credit card information—highlighting the value of the Digital Evidence Unit’s robust cell phone analysis program.
During an investigation in Pennsylvania, Forensic Computer Analysts identified a web server used by suspects in an alleged Click-N-Ship reshipping scheme. Analysts were able to forensically copy and then restore the data to standalone equipment so it could be reviewed without any loss of data integrity. The information helped Inspectors identify other suspects, gather suspects’ “private” communications, and collect crucial evidence, including suspects’ mailing labels.

Our Polygraph Examiners—just like those at the FBI, CIA, Secret Service, and the military—are trained at the National Center for Credibility Assessment, which is operated by the Defense Intelligence Agency and considered to be the best polygraph school in the country. In the polygraph chart shown below, a suspect is asked (at the section marked 4R), “Did you pry open that door at the Chapmanville Post Office?” The immediate surge in the green line, (indicating electrodermal activity from sweat glands in the hands), shows deception—and the suspect failed the polygraph. The Polygraph Examiner then interrogated the suspect, who confessed to the burglary.

Delivering Polygraph Services

Polygraphs are diagnostic instruments that produce a continuous record of physiological changes in the human body. The underlying principle is that an individual’s fear of detection and exposure when seeking to be deceptive produces physiological responses that are recorded via a polygraph and interpreted by an examiner.

The Postal Inspection Service’s Polygraph Examiners lend their investigative and technical expertise to interrogate criminal suspects and to screen new Postal Inspector applicants.

For example, after Postal Inspectors executed a search warrant at a home in St. Paul, MN, the resident admitted to ordering child pornography, although he denied ever having sexual contact with a minor. But a polygraph exam told another story: When confronted with the results, the man finally admitted having sexual contact with males less than 16 years old, including boys assigned to him as a Boy Scout Leader, as a Big Brother, and at an orphanage in Mexico.
The Postal Inspection Service operates two National Law Enforcement Communications Center (NLECC) facilities, at Dulles, VA, and Ft. Worth, TX. The facilities feature a national law enforcement radio network used primarily to provide communications support for Postal Inspectors and Postal Police Officers (PPOs). The radio network also supports interoperable radio communications between Postal Inspectors, Postal Police Officers, and other law enforcement agencies.

NLECC staff monitor intrusion-detection systems at Postal Service facilities and provide after-hours emergency phone coverage for all Postal Inspection Service offices. Staff members have access to law enforcement and intelligence information from such confidential sources as the National Crime Information Center (NCIC) and the International Justice & Public Safety Network (known as Nlets).

The NLECC design reflects critical post-9/11 coverage in support of the Postal Service’s Integrated Emergency Management Plan, which provides for continuity of operations for the Postal Service in the event of a power grid outage or regional or national disaster. Each NLECC facility has uninterruptible power supplies and diesel generators to provide power for extended coverage in the event of an electrical outage.

In FY 2010, NLECC staff reported these accomplishments:

- Addressed 52,000 phone calls related to emergency and law enforcement activities.
- Addressed 90,578 phone calls from postal employees and the general public.
- Supplied communications support for Postal Inspectors, PPOs, and local law enforcement groups for 84 burglaries, resulting in the apprehension of three suspects who were caught in the act of burglarizing Postal Service facilities.
Staff at the two NLECC facilities also provided communications support for these events:

- 276 requests for confirmations of wanted suspects.
- 1,777 incidents involving suspicious powders, unknown substances, suspicious mail, and other suspicious item events.
- 24 robberies.
- 88 accidents involving postal vehicles.
- 1,074 reports of unsecured facilities or mailboxes.

By setting up auto-dialing as a mandatory feature in alarm-system software for postal facilities, NLECC dispatchers can now more quickly notify first responders during emergencies, virtually eliminating dialing errors and yielding a more effective alarm-dispatch platform. The now near-immediate notification has resulted in successes like these:

- NLECC dispatchers contacted PPOs within two minutes of receiving the first of multiple burglary-alarm activations from the Postal Service’s Lakewood Station in Dallas, TX, in November 2009. PPOs discovered a broken rear window, took into custody a suspect caught in the act of burglarizing the station, and transported the suspect to a Postal Inspection Service facility in the area. When Inspectors interviewed the man, he confessed to the burglary.

- It took only 52 seconds for NLECC dispatchers to notify the Bakersfield, CA, Police Department of alarm activations at the Brundage Postal Station in December 2009. Officers and Postal Inspectors responded to the scene and took a suspect into custody. Inspectors later identified the man as a suspect in another Post Office burglary.

- NLECC dispatchers notified local police and Postal Inspectors in Amherst, MA, of a possible break-in at the Postal Service’s Amherst Finance Station in February 2010. Investigators gained entry to the facility less than a minute later and took one suspect into custody after a brief foot chase.
The concept of a “continuous improvement” culture is beginning to take root across the Postal Inspection Service, where eight executives have been certified as Lean Six Sigma (LSS) Executive Greenbelts and nine Postal Inspectors have been identified for Greenbelt training. By the close of FY 2010, the Postal Inspection Service’s LSS program had identified 26 projects, addressed 22 of them, and completed three.

With every LSS project, team members have the opportunity to shape processes, change their work environment, and adopt new LSS tools. They take this knowledge back to their duty locations and apply it in ways that will facilitate continuous improvement for their groups. A SIPOC chart—Suppliers, Inputs, Process, Outputs, and Customers—is used to identify the core elements of an LSS project. It depicts the flow of input from supplier to customer, and helps LSS teams focus on customer needs.

The Alarm Reduction Project now being implemented nationally has focused on reducing alarms triggered by employee errors. This joint effort involves experts from various Postal Service offices as well as Postal Inspection Service staff from its National Law Enforcement Communications Center, which monitors intrusion-detection systems at postal facilities. National deployment followed a 60-day test at 150 postal facilities in the Los Angeles area and a 30-day test at 120 facilities in the San Francisco area. Those tests showed the new alarm process consistently reduced employee error alarms by 60 percent from the previous fiscal year’s total; during 2009, more than 50,000 error alarms generated almost 30,000 dispatches by Postal Inspectors, Postal Police Officers, and local responders—at a cost of $1.4 million.

In another project, eight teams of Postal Inspectors and support staff assembled over two months during the summer of 2010 dissected specific types of case investigated by Inspectors. Their goals were to reduce duplication of effort, eliminate unnecessary steps, and automate repetitive actions as much as possible (steps known in LSS as eliminating waste, removing nonvalue-added work, and streamlining processes). Information gathered by the teams is being used to formulate new structures for case and database management.

Because process improvement is viewed as a continuous journey rather than a static, one-time effort, the Chief Postal Inspector continues to choose projects that focus on reducing workloads and increasing productivity.
Lean Six Sigma teams scrutinize processes by breaking them down into their simplest elements.

This is how we reduce duplication of effort, eliminate unnecessary steps, and streamline procedures—so we work leaner, faster, and smarter.

**ALARM REDUCTION PROCESS**

<table>
<thead>
<tr>
<th>SUPPLIERS</th>
<th>INPUT</th>
<th>PROCESS</th>
<th>OUTPUTS</th>
<th>CUSTOMERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faulty equipment</td>
<td>Triggered alarm</td>
<td></td>
<td>Asset/Resource security</td>
<td>Facility managers</td>
</tr>
<tr>
<td>Employee</td>
<td></td>
<td></td>
<td>Criminal action or no criminal action</td>
<td>Facility employees</td>
</tr>
<tr>
<td>Criminal</td>
<td></td>
<td></td>
<td>Faulty equipment data</td>
<td>Postal Inspection Service</td>
</tr>
<tr>
<td>Environment</td>
<td></td>
<td></td>
<td>Closed incident</td>
<td>NLECC</td>
</tr>
<tr>
<td>USPS customer</td>
<td></td>
<td></td>
<td>Recommendations</td>
<td></td>
</tr>
<tr>
<td>Construction changes</td>
<td></td>
<td></td>
<td>Notification</td>
<td></td>
</tr>
</tbody>
</table>

**NOTIFICATION**

- ALARM ACTIVATED

**DISPATCH**

- RESPONSE

**INVESTIGATE**

- INVESTIGATIVE FEEDBACK

**NOTIFY**

- NLECC

**RESOLUTION**
JURISDICTION AND LAWS

ASSAULTS
18 USC 111, 1114
The protection of Postal Service employees is one of our most important responsibilities. Postal Inspectors promptly investigate assaults and threats that occur while postal employees are performing official duties or as a result of their employment.

BOMBS
18 USC 1716
Although a rare crime, the mailing of bombs is given one of our highest investigative priorities due to the severe impact it can have on postal customers, employees, and operations.

BURGLARY
18 USC 2115
The Postal Service experiences only about 200 burglaries each year. Postal Inspectors have minimized losses through the use of updated security equipment and facility design.

CHILD EXPLOITATION
18 USC 1470, 2251, 2251A, 2252, 2252A, 2253, 2254, 2422, 2423, 2425
The Postal Inspection Service has long been recognized as one of the leading federal law enforcement agencies working to combat the production, distribution, receipt, and possession of child pornography and other crimes related to the sexual exploitation of children through the mail and the Internet.

CONTROLLED SUBSTANCES
21 USC 841, 843, 844
Postal Inspectors initiate investigations related to transporting and distributing narcotics through the mail or at postal facilities.

COUNTERFEIT STAMPS, MONEY ORDERS, AND RELATED CRIMES
18 USC 500, 501, 503, 1720
Postal Inspectors preserve public confidence in the mail by pursuing criminals who forge, alter, or counterfeit postage stamps, postal money orders, and other stamp products. The Postal Inspection Service helps train postal employees to recognize bogus postal money orders.

DESTRUCTION, OBSTRUCTION, AND DELAY OF MAIL
18 USC 1700, 1701, 1702, 1703
The Postal Inspection Service upholds federal statutes aimed at securing customers’ mail, including statutes related to the desertion, obstruction, delay, or destruction of mail. Postal Inspectors demonstrate their resolve by implementing mail security processes to ensure that customers receive their mail intact and free from outside interference.

ELECTRONIC CRIMES
18 USC 1029, 1030, 1037, 1343, 2701
Postal Inspectors protect customers from fraud schemes and other crimes that may occur online and involve the misuse of the mail or of the Postal Service. This includes using or selling stolen or counterfeit access devices, such as credit card numbers; using protected computers without proper authority or exceeding authorized access; using computer communications in a scheme to defraud; using a false identity when sending commercial e-mails to mislead or deceive recipients, as with spam; and unauthorized access to communications that are stored electronically via a communications service.
Postal Inspectors enforce more than 200 federal laws through investigations of crimes that may adversely affect or fraudulently use the U.S. Mail, the postal system, or postal employees. Here are some of the agency’s most important areas of jurisdiction.

**EXTORTION**  
18 USC 873, 876, 877  
Postal Inspectors investigate extortion and blackmail when demands for ransoms or rewards are sent through the U.S. Mail. They strictly enforce laws prohibiting mail that contains threats of kidnapping, physical injury, or injury to the property or reputations of others.

**FORFEITURE**  
18 USC 981, 982  
Postal Inspectors use criminal and civil forfeiture statutes, when appropriate, to seize assets associated with criminal acts.

**IDENTITY FRAUD**  
18 USC 1028  
The Postal Inspection Service is a leading federal law enforcement agency in the investigation of identity takeovers.

**LOTTERIES**  
18 USC 1301, 1302, 1303 and 39 USC 3005  
Postal Inspectors protect consumers by strictly enforcing all laws related to importing, transporting, and mailing lottery tickets. Under the false representations and lottery statute (3005), Postal Inspectors are authorized to instruct postmasters to withhold from delivery and return to sender any mail that violates the law.

**MAIL FRAUD**  
18 USC 1341, 1342, 1345  
and 39 USC 3005, 3007  
The Postal Inspection Service is committed to protecting postal customers from misuse of the mail. Postal Inspectors place special emphasis on mail fraud scams related to advance fees, boiler rooms, health care, insurance, investments, deceptive mailings, and other consumer fraud, especially when it targets the elderly or other vulnerable groups.

**MAIL OR MAILBOX DESTRUCTION**  
18 USC 1705  
The Postal Inspection Service is committed to ensuring the safety of the nation’s mail by securing letter boxes or other receptacles for U.S. Mail. To this end, Postal Inspectors aggressively pursue individuals who willfully or maliciously injure or destroy such receptacles.

**MONEY LAUNDERING**  
18 USC 1956, 1957  
Postal Inspectors aggressively investigate criminals who attempt to conceal the proceeds of illegal acts through monetary transactions. They identify and seize criminals’ assets, denying violators the proceeds of their crimes.

**OBSCENITY AND SEXUALLY ORIENTED ADVERTISING**  
18 USC 1461, 1463, 1735 and 39 USC 3010  
Postal Inspectors follow court-established guidelines to uphold obscenity standards, which prohibit “obscene, lascivious, indecent, filthy, or vile” mailings. Customers who wish to halt mailings of sexually oriented advertisements or similar solicitations may complete and submit PS Form 1500, available at Post Offices or online.

**ROBBERY**  
18 USC 2114  
Postal Inspectors respond promptly to robberies of postal employees and postal contractors. They work to prevent robberies through the use of security equipment and improved postal procedures.

**THEFT OF MAIL**  
18 USC 1708, 1709  
Postal Inspectors invest significant resources into the investigation of mail theft by criminals, including Postal Service contractors who transport mail to postal facilities.
“The protection offered by Postal Inspectors for our mailings can’t be duplicated by any other mail service.”

— KAREN TRIMMER, SENIOR BUSINESS ANALYSIS MANAGER, JPMORGAN CHASE
### CRIMINAL STATISTICS FY 2010

<table>
<thead>
<tr>
<th>Investigation Initiated</th>
<th>Arrests</th>
<th>Indictments</th>
<th>Convictions*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Theft by Nonemployees and Contractors</td>
<td>1,702</td>
<td>2,775</td>
<td>994</td>
</tr>
<tr>
<td>(includes theft, possession of stolen mail, and identity theft)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspicious Substances</td>
<td>33</td>
<td>18</td>
<td>11</td>
</tr>
<tr>
<td>(includes non-threatening, hazardous, and hoax CBRN**)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspicious Items</td>
<td>31</td>
<td>35</td>
<td>12</td>
</tr>
<tr>
<td>(includes non-threatening items, bombs, threats, hoaxes, and explosive material)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonmailable, Restricted, and Perishable Matter</td>
<td>105</td>
<td>75</td>
<td>36</td>
</tr>
<tr>
<td>(includes firearms, weapons, intoxicants, extortion threats, and miscellaneous matter)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assaults and Threats</td>
<td>508</td>
<td>229</td>
<td>40</td>
</tr>
<tr>
<td>(includes threats and assaults against on-duty postal employees and homicide)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Robbery</td>
<td>75</td>
<td>61</td>
<td>37</td>
</tr>
<tr>
<td>Burglary</td>
<td>129</td>
<td>62</td>
<td>24</td>
</tr>
<tr>
<td>Mailing of Controlled Substances</td>
<td>1,075</td>
<td>1,322</td>
<td>481</td>
</tr>
<tr>
<td>(includes narcotics, steroids, drug-related proceeds, and drug paraphernalia)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mail Fraud</td>
<td>589</td>
<td>1,007</td>
<td>903</td>
</tr>
<tr>
<td>Child Exploitation, Mailing of Obscene Matter, and Sexually Oriented Advertisements</td>
<td>118</td>
<td>115</td>
<td>70</td>
</tr>
<tr>
<td>Revenue Fraud</td>
<td>334</td>
<td>68</td>
<td>39</td>
</tr>
<tr>
<td>Money Laundering</td>
<td>154</td>
<td>203</td>
<td>71</td>
</tr>
<tr>
<td>(includes postal money orders)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vandalism and Arson</td>
<td>68</td>
<td>42</td>
<td>2</td>
</tr>
<tr>
<td>Workers’ Compensation Fraud</td>
<td>1,091</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>6,013</td>
<td>6,013</td>
<td>2,720</td>
</tr>
</tbody>
</table>

* Convictions include pretrial diversions and may be related to cases from prior reporting periods.
** CBRN refers to chemical, biological, radiological, and nuclear.
Think of us the next time you place a stamp on an envelope or mail a parcel.

As your mail is hurried to its destination—safely and securely—know that we are protecting you.

It’s all included in the price of postage.