Testimony of:
Timothy J. Menke
Deputy Inspector General for Investigations
Office of Inspector General, U.S. Department of Health & Human Services

OIG'S LAW ENFORCEMENT ACTIVITIES TO COMBAT MEDICARE AND MEDICAID FRAUD

Good morning Chairman Scott, Ranking Member Gohmert, and distinguished Members of the Subcommittee. I am Timothy Menke, Deputy Inspector General for Investigations at the U.S. Department of Health & Human Services' (HHS) Office of Inspector General (OIG). I thank you for the opportunity to discuss OIG's health care anti-fraud strategy, focusing primarily on our law enforcement activities to combat Medicare and Medicaid fraud.

OIG's Role and Partners in Protecting the Integrity of Medicare and Medicaid

OIG is an independent, nonpartisan agency committed to protecting the integrity of more than 300 programs administered by HHS. Approximately 80 percent of OIG's resources are dedicated to promoting the efficiency and effectiveness of the Medicare and Medicaid programs and protecting these programs and program beneficiaries from fraud and abuse.

OIG employs more than 1,500 dedicated professionals, including a cadre of nearly 400 highly skilled criminal investigators trained to conduct criminal, civil, and administrative investigations of fraud, waste, and abuse related to HHS programs and operations. Our special agents have full law enforcement authority to effectuate the broad range of available law enforcement actions, including the execution of searches and making arrests. We utilize state-of-the-art technologies and a wide range of law enforcement tools in carrying out these important responsibilities.

Thanks to the hard work of our employees, in fiscal year (FY) 2009, OIG's enforcement efforts resulted in over 670 criminal actions, of which 515 involved heath care fraud; over 362 civil actions (355 involved health care fraud); and realized nearly $4 billion in settlements and court-ordered fines, penalties, and restitution, approximately 75 percent of which involved health care fraud. Additionally, OIG excluded over 2,500 providers from Federal health care programs.

OIG is not alone in the fight to combat fraud and protect the integrity of Federal health care programs. We work closely with the Department of Justice (DOJ), our Federal, State, and local law enforcement partners, and our colleagues at the Centers for Medicare & Medicaid Services (CMS) and the Food and Drug Administration. Additionally, commercial and private insurance entities and trade associations, such as the National Health Care Anti-Fraud Association (NHCAA), are also involved in the identification and prevention of health care fraud. OIG conducts joint investigations with law enforcement agencies where there is concurrent jurisdiction and where sharing expertise or authority will lead to the best results possible. In FY 2009, OIG worked over 2,700 cases with our law enforcement partners on the Federal, State, and local levels, including over 980 cases with State Medicaid Fraud Control Units (MFCU).

OIG's partnerships extend to one of the Administration's signature initiatives, the Health Care Fraud Prevention and Enforcement Action Team (HEAT). This is a joint effort by HHS and DOJ to leverage resources, expertise, and authorities to prevent fraud and abuse in Medicare and Medicaid. The HEAT initiative, established by Secretary Sebelius and Attorney General Holder in May 2009, is an unprecedented partnership that brings together senior officials from both Departments with the stated goals of sharing information, spotting fraud trends, coordinating prevention and enforcement strategies, and developing new fraud prevention tools. OIG contributes its expertise to HEAT by analyzing data for patterns of fraud; conducting investigations; supporting Federal prosecutions of providers who commit criminal and civil fraud; and pursuing administrative remedies, including program exclusions. OIG also makes recommendations to HHS to remedy program vulnerabilities and prevent fraud and abuse.

Overview of the Referral Process

OIG receives information about potential instances of fraud, waste and abuse through many sources. One source of information is the OIG Hotline. The Hotline receives and manages complaints of fraud, waste, abuse, and mismanagement related to HHS programs by way of phone, mail, fax, or email. In FY 2009, the OIG Hotline received approximately 5,000 complaints related to health care fraud. OIG also receives information in the form of correspondence from Congress, citizens, and a broad range of agencies. Information regarding health care fraud may also be received by our various offices directly from HHS operating divisions, as well as from other Federal, State and local law enforcement agencies.

A significant number of referrals come from official qui tam[1] notifications from DOJ. OIG also receives notification of Voluntary Self Disclosures sent from various health care related entities. OIG Regional Offices receive case referrals screened and prepared by the CMS Program Safeguard, Zone Program Integrity, and other integrity contractors and occasionally receive information obtained directly from CMS's Program Integrity staff. OIG is very active in internal working groups that target specific areas of health care issues, and has established liaisons with other agencies through health care fraud working groups sponsored by district-specific U.S. Attorneys Offices.

Additionally, OIG develops cases internally through its various components. The Office of Investigations (OI) through its outreach efforts with not only other law enforcement and government organizations, but also community contacts, develops investigative leads. Our Office of Audit Services refers complaints to OI based on its audit verification work. OI has initiated investigations based on the Office of Evaluation and Inspections identification of fraud trends.

Range of Investigations

[1] The qui tam provisions of the Federal False Claims Act allow a private person, known as a "relator," to bring a lawsuit on behalf of the United States, where the private person has evidence of fraud against the Government, and to share in a portion of the funds recovered.

From street gang members to corporate officers, our investigations are uncovering a wide range of individuals and entities committing health care fraud. The profitability, ease of entry, and lower criminal penalties for health care related crimes attract criminals to health care fraud. Unfortunately, we also see some legitimate providers engaging in health care fraud. Below are examples of various fraud schemes we have encountered.

In 2009, OIG, along with our law enforcement partners, successfully completed one of the largest Federal Government settlements in history. Pfizer Inc, a drug manufacturer, and its subsidiary, Pharmacia & Upjohn Company, Inc. entered a $2.3 billion global resolution with the Federal Government and participating States. The agreement settled charges that Pfizer promoted four drugs, including its pain drug Bextra, for uses not approved by FDA and that the company paid kickbacks to health care professionals to induce them to prescribe Pfizer drugs. In its plea agreement, Pfizer's subsidiary admitted that it promoted Bextra for unapproved uses and at unapproved dosage levels. Pfizer also entered into a comprehensive 5-year Corporate Integrity Agreement (CIA) with OIG, which requires procedures and reviews to be put in place to avoid and promptly detect fraud or misconduct. Two corporate officers were charged criminally for their role in this matter.

In Southern California, an individual set out to defraud the Medicare program by establishing multiple fraudulent durable medical equipment (DME) companies. The owner used primarily members of a street gang as nominee owners of his DME companies. He paid the gang members approximately $5,000 each to establish bank accounts and fill out the Medicare paperwork. The nominee owners submitted claims for reimbursement to Medicare for power wheelchairs and orthotic devices that were not medically necessary or legitimately prescribed by a physician. To date, nine of the gang members and associates have been indicted for charges including health care fraud and providing false statements to government agencies. Not only is this investigation an example of one of the more prevalent fraud schemes that we are seeing, but also it highlights the increasing number of violent criminals entering the health care fraud arena. The criminal records for the gang members involved in this fraud ranged from assault on a peace officer to drug trafficking.

Another example of egregious health care fraud that OIG has investigated is the "Small Smiles" case. FORBA Holdings, LLC (FORBA), a management company operating Medicaid pediatric dental clinics, recently agreed to pay $24 million plus interest and enter into a 5-year quality-of-care CIA to settle allegations that it performed unnecessary and often painful services on children to maximize Medicaid reimbursement. FORBA manages a chain of 68 pediatric dental clinics in 22 States and the District of Columbia commonly known as "Small Smiles Centers." The investigation revealed that among other things, FORBA allegedly caused the submission of claims for reimbursement for dental services that either were not medically necessary or did not meet professionally recognized standards of care. Such services billed to the Medicaid programs included performing pulpotomies (baby root canals), placing multiple crowns, administering anesthesia, performing extractions, and providing fillings and/or sealants. This investigation involved OIG, the Federal Bureau of Investigation, and the National Association of MFCUs.

Our investigations have shown that there has been an increase in organized criminal enterprises within the health care fraud arena. Common elements of criminal enterprises include:

- use of consultants to start a company and obtain a Medicare billing number;
- use of "store fronts" – places made to look like legitimate medical companies;
- use of "false fronts" – billing for companies that do not exist or have a false address;
- use of straw or nominee owners and middlemen to protect the identities of real owners;
- association with medical identity theft rings to obtain stolen physician and patient identification numbers;
- use of "cappers," or recruiters, to recruit beneficiaries at rehabilitation facilities, soup kitchens, and senior centers for the use of their Medicare or Medicaid cards, and
- cooperation with other criminal enterprises, such as check cashing and money laundering rings.

Sham DME companies, home health companies, clinics and diagnostic laboratories are common schemes in criminal enterprises. Health care fraud is attractive to organized crime because: (1) the penalties are lower than those for other organized-crime-related offenses (e.g., offenses related to illegal drugs); (2) there are low barriers to entry (e.g., a criminal can obtain a supplier number, gather some beneficiary numbers and bill the program); (3) schemes are easily replicated; and (4) there is the perception of the low risk of detection.

An example of a criminal enterprise case involves Alain Amador who was sentenced to 52 months of incarceration and ordered to pay $3,928,552 in restitution following his guilty plea to conspiracy to commit health care fraud. Amador and his co-conspirators set up a series of fake medical clinics that existed in name only. Amador, who has a nursing degree, was instrumental in leasing space in the names of the companies, opening bank accounts, incorporating the companies, and obtaining Medicare billing numbers for the companies. The conspirators also improperly obtained identity information of legitimate doctors and Medicare patients. In fact, the investigation initiated with a complaint by a physician who had provided the conspirators with her Medicare provider number when applying for a medical director position at a clinic that they were allegedly opening. The stolen information was used to bill Medicare for infusion therapy services that were not rendered.

Criminal Statutes and Applicable Laws

There are a number of criminal laws that our agents and prosecutors have utilized successfully in strike force and other health care fraud cases. These include, most typically, Health Care Fraud (18 U.S.C. § 1347), which generally provides for prison sentences of up to 10 years, and can result in a sentence of up to 20 years for violations involving serious bodily injury and up to life if the action results in a death. Wherever possible, we have also supported criminal forfeiture of the stolen Medicare funds under the Criminal Forfeiture statute (18 U.S.C. § 982).

To attack more complicated schemes, in addition to the health care fraud statute cited above, our teams have utilized Conspiracy to Commit Health Care Fraud (18 U.S.C. § 1349), and Conspiracy (18 U.S.C. § 371) charged in combination with False, Fictitious, or Fraudulent Claims (18 U.S.C. § 287). For cases involving money laundering, we have on occasion pursued additional charges under Laundering of Monetary Instruments (18 U.S.C. § 1956). Many schemes also involve the solicitation or receipt of illegal kickbacks, which are charged under Criminal Penalties for Acts Involving Federal Health Care Programs (42 U.S.C. § 1320a-7b (b)).

Finally, in cases involving identity theft, we have occasionally pursued charges under 18 U.S.C. § 1028A (Aggravated Identity Theft), which provides for an additional term of imprisonment of 2 years that generally runs consecutively with any sentence imposed for any other related crimes.

In all of these cases, our agents work with prosecutors to develop facts supporting appropriate enhancements at sentencing.

Investigative Strategies

Strike Forces

The Medicare Fraud Strike Force, an antifraud effort in geographic areas at high risk for Medicare fraud, has changed the way health care fraud cases are investigated and prosecuted. Strike Force cases focus on the development and implementation of a technologically sophisticated and collaborative approach.

The typical Strike Force case differs from our traditional health care fraud investigations in the complexity and nature of the scheme. Our traditional health care fraud investigations often rely upon individuals with knowledge of the scheme, including corporate insiders. In contrast, Strike Force cases are data driven, using technology to pinpoint fraud hot spots through the identification of unexplainable billing patterns as they occur. Substantiating the allegation of fraud is more difficult when dealing with individuals as opposed to verifying the accuracy of evidence obtained directly from Medicare billing information. Also, in traditional health care cases the subjects of the investigations often provide some level of legitimate services. The majority of subjects in Strike Force cases are engaging in 100 percent fraud, i.e., not providing any legitimate services to beneficiaries. These differences allow Strike Force cases to be completed more quickly. Strike Force investigations are typically fully adjudicated in about 1 year, whereas traditional investigations can take up to 3 years.

OIG and DOJ first launched their Strike Force efforts in 2007 in South Florida using the expertise of staff from OIG, DOJ and the U.S. Attorney's Office for the Southern District of Florida, the FBI, and CMS to identify, investigate, and prosecute DME suppliers and infusion clinics suspected of Medicare fraud. Building on the success in South Florida, the Strike Force model was expanded to Los Angeles in March 2008. Today, Strike Force operations are in place in seven locations: South Florida, Los Angeles, Houston, Detroit, Brooklyn, Tampa, and Baton Rouge.

We believe that our Strike Forces have had a marked sentinel effect. Though deterrence is difficult to quantify, we have empirical evidence that our Strike Force model for investigating and prosecuting health care fraud has resulted in reductions in improper claims to Medicare. Claims data showed that during the first 12 months of the Strike Force (March 1, 2007, to February 29, 2008), claim amounts submitted for DME in South Florida, a particularly hot spot of DME fraudulent activities, decreased by 63 percent to just over $1 billion from nearly $2.76 billion during the preceding 12 months.

As of January 30, 2010, our Strike Force efforts nationwide have charged over 500 defendants, obtained over 270 convictions, resulted in the sentencing of over 200 defendants, and secured over $240 million in court-ordered restitutions, fines, and penalties.

In one Miami Strike Force case, two brothers were indicted for conspiring to submit approximately $110 million in false and fraudulent claims to the Medicare program for HIV infusion services allegedly provided at 11 corrupt HIV infusion clinics that they owned and controlled. As part of the scheme, the defendants referred Medicare beneficiaries to the clinics and directed that the beneficiaries be paid kickbacks to induce them to claim they received legitimate services at the clinics when in fact the HIV infusion services either were not provided or were not medically necessary.

The Strike Force model is especially effective for investigating and prosecuting fraud committed by sham providers masquerading as legitimate providers. This fraud is viral and migratory. However, that is only one model of health care fraud. Major corporations and institutions, such as pharmaceutical manufacturers, hospitals and nursing facilities also commit fraud, often on a grand scale. These corporate and institutional frauds often involve complex kickbacks, accounting schemes, illegal marketing, and physician self-referral schemes. These cases necessitate different, and often more laborious, investigative techniques to unravel the complex fraud schemes and build strong cases.

Importance of Real-Time Data Access

The Strike Forces are designed to target fraud in areas identified as being at high risk for and having high concentrations of health care fraud. OIG is implementing a new paradigm in fighting fraud by using data analysis to swiftly identify, investigate, and prosecute health care fraud perpetrators. Strike Force investigations are data driven and target individuals and groups that are actively involved in ongoing Medicare fraud schemes.

Real-time access to data is critical to the success of the HEAT Strike Force initiative. Over the last several months, representatives from OIG, CMS, and DOJ have explored ways to improve access to CMS claims data. Much of our attention has been focused on obtaining real-time data. To date, we have established limited access to real-time claims data but we are continuing to work to improve our access to these data, increase the number of investigators who have access, and expand access across all parts of the Medicare program. In addition to having access to real-time data, it is also important that we expand our access to CMS systems offering advanced analysis and query tools that can be employed in mining a comprehensive national Medicare claims database. Since the start of HEAT, OIG has sent more than 130 investigators and analysts to

claims database training and we anticipate each of them having access to the database by mid-March 2010. Other projects that are in progress at this time include:

- developing standardized summary reports for claim dollars submitted for payment, denied for payment, and allowed by Part A and B providers;
- improving investigators' access and ability to analyze Medicare Part D prescription drug event data;
- developing a more efficient and less timely process for obtaining access to CMS contractor support for trials; and
- establishing a cross-government data intelligence sharing workgroup to share ideas and success stories.

Real-time data access is also important in our traditional health care fraud investigations. There are many investigative activities performed throughout an investigation that require the agent to gather all available information to effectively plan and conduct the operation. In an effort to keep up with the criminals, immediate access to the most current claims information gives law enforcement an important advantage when interviewing witnesses and efficiently identifying subjects for investigation.

Additionally, real-time data access would enable us to more efficiently conduct field surveillance, electronic monitoring, and issue search and arrest warrants. The more current the data, the more effective our agents can be when:

- confronting a witness who may be lying or withholding information;
- identifying relevant parties, locations, and times to conduct surveillance or electronic monitoring operations in order to have the best chance to observe an ongoing criminal operation;
- planning a search warrant so that we can quickly and accurately locate evidence of a crime (including evidence that no service was provided) before perpetrators destroy, alter, or manufacture information; and
- planning an arrest warrant so that we can quickly determine the location of a subject before the subject is alerted to our investigation and has an opportunity to flee or prepare for our arrival if the subject does not intend to cooperate.

The more effective we are when conducting these operations, the less likely there will be any surprises. This helps to ensure the safety of our agents and others whom we encounter during these operations. It also increases the likelihood that our cases will succeed at prosecution.

In addition to using data to more efficiently conduct our investigations, OIG is also using data to take a more strategic approach to identifying fraud. In 2009, OIG organized the cross-component Advanced Data Intelligence and Analytics Team (Data Team) to support the work of HEAT. The Data Team includes OIG special agents, statisticians, programmers, and auditors. Together, the Team brings a wealth of experience in utilizing sophisticated data analysis tools combined with criminal intelligence gathered directly from special agents in the field to more quickly identify ongoing health care fraud schemes and trends.

The selection of Strike Force city locations is also data driven. To support this, OIG's Data Team analyzes Medicare claims data and the prevalence of unusual Medicare billing patterns in

various metropolitan areas across the United States. Specifically, the team identifies Medicare fraud "hot spots" on a national level, narrowing those results to regional trends, and then reducing those selections to specific metropolitan areas. Utilizing the findings of the Data Team, the HEAT Operations Committee was able to more effectively strategize in determining the next locations for Strike Force operations.

OIG is also capitalizing on cutting-edge electronic discovery tools to maximize investigative efficiency in the processing and review of voluminous electronic evidence obtained during the course of our health care fraud investigations. This technology is Web-based and has been made available to OIG investigators throughout the organization to increase investigative efficiency and effectiveness. OIG was the first Federal law enforcement agency to implement this technology. It enables OIG to analyze large quantities of email or other electronic documents more efficiently, and to associate or link emails contained in multiple accounts based on content and metadata. Recently, OIG has expanded the use of this technology by making it available to our external law enforcement partners for use in joint investigations. This effort strengthens OIG's relationships with partner law enforcement agencies and allows for much greater collaboration. Because the technology is Web-based and can be accessed securely over the internet, investigators can use this tool from anywhere in the country.

Conclusion

The examples that I have discussed today are critical aspects of a multi-departmental effort to protect the health, vitality, and integrity of Federal health programs, as well as protect the finite resources dedicated to pay for these services and programs. OIG is committed to investing in program integrity efforts in order to send a clear message that criminal fraud in our Federal health care programs will not be tolerated.

By attacking fraud vigorously, wherever it exists, we all stand to benefit. Medicare Trust Fund resources will be protected and remain available for their intended purposes. Medicare dollars that have gone to fraudulent suppliers will instead be available for legitimate businesses whose purpose is to serve the critical health care needs of our program beneficiaries. And most importantly, we can ensure that seniors and persons with disabilities receive the necessary supplies and care they need to stay healthy, so as to enjoy enhanced wellbeing and quality of life.

Thank you for the opportunity to discuss our law enforcement efforts and strategies to protect the integrity of Federal health care programs.