

Good afternoon Chairman Obey, Ranking Member Tiahrt and distinguished Members of the Subcommittee. I am Omar Perez, Special Agent with the U.S. Department of Health and Human Services' (HHS) Office of Inspector General (OIG). I am stationed in the Miami Regional Office, and I am a member of one of the Medicare Fraud Strike Force teams. I am honored for the opportunity and invitation to discuss OIG's efforts in combating Medicare and Medicaid fraud.

I am here this afternoon to tell you what I experience as a criminal investigator who is on the front-line in the fight against criminal health care fraud. Although the vast majority of Medicare providers are honest, my job is to focus on the ones who steal from the program. I am actively engaged in criminal health care fraud investigations, executing search and arrest warrants, seizing bank accounts, and providing Grand Jury testimony in the pursuit of criminal indictments.

In Miami, Medicare fraud is not only perpetrated by independent, scattered groups, but also by competitive, organized businesses complete with hierarchies and opportunities for advancement. Medicare fraud is discussed openly on the streets and is accepted as a safe and easy way to get rich quick.

Who commits this fraud? People from all walks of life – they say it's easy money and it's safer than dealing drugs. I see people who never finished high school living lavish lifestyles, making anywhere from \$100,000 to millions of dollars a year by committing Medicare fraud. The money involved is staggering. We see business owners, health care providers and suppliers, doctors, and Medicare beneficiaries participate in the fraud. We see drug dealers and organized criminal enterprises participate in the fraud.

How much money is involved? Too much. As an example, I will tell you a little later about one of my cases – in which \$1.8 million was billed to Medicare in a two and a half week time period.

In my testimony today, I will describe a typical Medicare fraud scheme that we investigate in Miami. I will then provide an overview of the Miami Strike Force investigative approach from an agent's perspective. I will share examples of Miami Strike Force success stories. Finally, I will discuss the evolution of fraud in South Florida.

COMMON DURABLE MEDICAL EQUIPMENT FRAUD SCHEMES PRE-STRIKE FORCE

Prior to the start of the Strike Force, South Florida was riddled with sham durable medical equipment (DME) companies. Some of these companies started out as legitimate operations with a Medicare billing number; however, they were unsuccessful as the market was saturated with illegitimate DME suppliers. As a result, these companies were sold all too often and their new owner(s) had one idea in mind: steal from Medicare.

Once in the hands of these criminals, these companies no longer provided legitimate services. In order to perpetrate the fraud, “nominee owners”¹ were recruited. The names of these nominee owners were placed on corporate documents, lease agreements, and corporate bank accounts. Those perpetrating the fraud then obtained lists of stolen Medicare beneficiary information which were compiled by individuals with access to patient information, such as employees of hospitals, clinics, and physicians’ offices. The criminals also obtain lists of stolen physician Unique Physician Identification Numbers (UPIN), assigned to physicians by the Centers for Medicare & Medicaid Services (CMS) which are essential to the completion of a Medicare claim for reimbursement. With these two key pieces of information, the nominee owners would submit fraudulent claims to Medicare for DME that was never provided. The types of equipment ranged from nebulizers and corresponding medications, to incontinence supplies to motorized wheelchairs.

Once CMS paid the claims and deposited money into the company’s bank account, it was withdrawn within days using multiple check cashers. The idea was to deplete the account so that once Medicare discovered the fraudulent billing, which could take 6 months to 1 year, there would be no money in the account.

MIAMI STRIKE FORCE APPROACH TO COMBATING FRAUD

The DME fraud schemes described above were executed within a matter of months. After billing Medicare for millions of dollars, companies would change ownership, bill Medicare again for millions of dollars, close and simply take over another company and repeat the process in another location. By the time traditional investigative referral methods came to fruition, criminals had absconded with millions of tax payer dollars.

A streamlined investigative approach was created for Strike Force investigations. The Strike Force model is a collaboration between the Department of Justice (DOJ) and HHS. Each Strike Force team includes agents from HHS OIG and the Federal Bureau of Investigation, as well as attorneys from DOJ. The teams are supported by investigative analysts as well as CMS program experts and contractors. Miami has five Strike Force teams dedicated to investigating HIV infusion therapy fraud, physical

¹ A nominee owner is an individual who is recruited and paid by the true owner to be the owner of record for a DME company. This process occurs to protect the identity of the true owner.

therapy/occupational therapy fraud, DME fraud, and pharmacy fraud. There are also three teams in Miami dedicated to investigating Medicare Part A Home Health Agency fraud.

The individual investigations generally follow a model that has proved highly successful in these fraud schemes. The model includes the following steps: (1) analyze and evaluate claims data; (2) obtain the Medicare enrollment application; (3) identify the medical biller; (4) identify and obtain bank information; and (5) identify the “true” owner of the clinic and/or DME company that is under investigation.

Analyze and evaluate claims data

Strike Force team members receive Medicare billing data gleaned from a wide variety of CMS data systems. We analyze the data to identify aberrant billing patterns. Before Strike Force teams were initiated, the referrals we received contained billing data that was typically between 6 months and 1 year old. Today, the data we receive provides billing information that is only 2 to 3 weeks old. In South Florida, criminals can receive several hundred thousand dollars in fraudulent payments within a matter of weeks. The ability to retrieve real-time data, meaning being able to access claims data within hours of the claims being submitted, would allow us to potentially obtain evidence immediately to substantiate fraudulent activity, thus stopping the payment of a significant amount of money and catching the criminals before they and the money disappear. What we have now is progress and better than what we had even a year ago, but with new resources I am hopeful for even more improvement.

The claims information can help us identify important information in assessing whether a fraudulent scheme is underway, including:

- total amount paid
- dates of service
- referring/ordering physicians
- beneficiaries
- claim dates
- types of procedures billed
- place of service
- provider banking information
- ownership status.

This process is called developing an investigative snapshot² of the suspected fraudulent activity.

Obtain the Medicare enrollment application and other data

² “Snapshot” refers to an excerpt of a provider’s or supplier’s billing history that includes total amount billed, claims denied, patient name, referring physicians, procedural codes billed, dates of service and place of service.

Obtaining the Medicare enrollment application is extremely important because it identifies the registered owner, his or her financial institution, and the authorized medical billing representative. For investigators, this information can generate countless leads to other co-conspirators involved in the fraudulent activity.

Identify the Medicare medical biller

The Medicare billing process begins when the medical biller electronically submits the patient's information to a Medicare claims contractor for processing and reimbursement. The medical biller could be an employee of the fraudulent company and/or a contracted third party. It is important for investigators to interview the medical biller to determine his or her level of complicity, if any, and identify who provided the billing information.

Identify the bank account and financial institution of the fraudulent business

A critical investigative step is determining the true owner of the fraudulent provider's bank account. In many instances, the true owner is not the individual who opened the bank account, withdrew or transferred funds, and/or cashed the Medicare checks. It is a significant investigative step for investigators to identify and interview all individuals with signatory control over these accounts.

Identify the "true" owner of the clinic and/or DME company

Strike Force members utilize commercial databases, bank account data, and informants in an effort to identify the true owners of the company. Once the true owner is identified, Strike Force members will attempt to interview the true owner in furtherance of the investigation.

Typically, a nominee owner is paid \$10,000 to \$20,000 for his or her role. Our sources have told us that nominee owners have been recruited in other countries and travel to South Florida solely for this purpose. After being paid, they return to their native countries.

MIAMI STRIKE FORCE SUCCESS STORIES

To highlight the successes of our streamlined investigative strategy, I offer the following examples:

My Strike Force team discovered, through data analysis, an aberrant billing pattern for City Wide M.S. Corp (City Wide), a DME company. City Wide had just been purchased by Rodolfo Gonzalez . In that month alone, Gonzalez had caused approximately \$1.8 million in fraudulent claims to be submitted to Medicare. (Prior to the change of ownership, City Wide was submitting claims of nominal value.) The Strike Force team members contacted the bank where City Wide received its electronic deposits and learned

that over \$100,000 was in the account. One day later, agents were advised that someone was trying to deplete the account. We rushed to the bank but did not find the individual there. Immediately, we went to Gonzalez's home to interview him. Prior investigative steps had revealed that the highest referring physician identified in City Wide's claims data attested he did not know the patients billed under his UPIN nor had the physician ordered the type of equipment for which City Wide was billing. When confronted, Gonzalez admitted he owned the company and was an authorized signer on the account. In an attempt to minimize his involvement in the fraud, he voluntarily forfeited the funds in the account to the Government that day. Immediately after we interviewed Gonzalez, City Wide Medicare claims ceased. Gonzalez was indicted and charged with conspiracy, healthcare fraud, and aggravated identity theft. He was found guilty by a trial jury of conspiracy to commit healthcare fraud, sentenced to 48 months incarceration, and ordered to pay \$325,442 in restitution.

In a second illustrative case, my Strike Force team received a phone call from a financial institution advising that Reinel Pulido was inquiring about a hold placed on his company's corporate bank account. Soroa Medical was a DME company that Pulido claimed he was operating for a friend. The company submitted over \$15.6 million in fraudulent claims and was reimbursed \$1,565,410. Pulido was interviewed at the bank and admitted to being recruited to place his name on all the documents related to Soroa Medical. He was paid approximately \$50,000 for becoming the nominee owner. Strike Force agents confronted Pulido with the evidence and he voluntarily forfeited the \$75,910 in his company's bank account. Pulido was arrested immediately. He was sentenced to 36 months incarceration and was ordered to pay \$1,565,410 in restitution.

THE EVOLUTION OF FRAUD IN SOUTH FLORIDA

In many instances, criminals have shifted their schemes from purchasing legitimate DME companies to instead establishing storefront shams. The storefronts are set up by criminals who have the required equipment to pass Medicare onsite inspections. Once the Medicare provider number has been issued, the individuals pick up their equipment and all that remains is an empty storefront.

Some criminals create additional layers to shield the true owners to counter Strike Force tactics. Prior to Strike Force operations, the true owner was most likely an associate of the nominee owner. Now there are many levels to a criminal enterprise; each level operating independently of the others but controlled by the same person.

We have also found that criminals are now often migrating to other services within the Medicare program to perpetrate their fraud. Other services impacted include: home health, community mental health, and physical therapy/occupational therapy. Historically, Medicare beneficiaries and physicians were not involved in criminal enterprise. Now we are finding that in many cases both are getting paid to participate in fraud.

CONCLUSION

The investigative approach and success stories referenced today represent the dedication and commitment of all OIG special agents and their collaborative partners in the fight against criminal fraud within the Medicare and Medicaid insurance programs. The HEAT initiative is an example of how combined resources, technology and collaboration can be synthesized to combat healthcare fraud in an effort to protect one of the most vulnerable segments in our society.

Thank you for the opportunity to discuss Strike Force operations in South Florida and the strategies and investigative methods utilized to protect the interest of all taxpayers. I would be happy to answer any questions that the Subcommittee may have.