FASTCOMPANY.COM
Where ideas and people meet
Article location:http://www.fastcompany.com/magazine/161/medical-fraud
November 7, 2011
Tags: Ethonomics, Work/Life, Magazine, medicare fraud

Cracking Down On $70 Billion Worth Of Medicare Fraud

By Tristram Korten

Photo by Edward Linsmier

Special agent Brian Hill pulls his car alongside the Goodyear automotive shop on East First Avenue in Hialeah, a heavily Cuban city of squat industrial buildings on the outskirts of Miami, and gazes across the street toward a strip mall. From the car, Hill and his partner eyeball the line of storefronts: a pizza place, a barbershop, an eyeglass store. Then they find what they're looking for--Elbia's Pharmacy, a six-year-old business that was sold a few weeks earlier and has just reopened. Hill puts the car in park and keeps the motor running. It promises to be a sweltering day, so the air conditioning needs to stay on. The two men get out th[illegible]ulars and settle in for a long wait. Both have Glock 40-caliber semiautomatics holstered on th[illegible]hey have coffee and Mountain Dew handy. On the backseat, within easy reach, are two bull[illegible] vests.

H[illegible]it Medicare Fraud In Six Easy Steps [1]

A few days before, a tipster had telephoned Hill, a special agent with the Office of Inspector General (OIG) for the U.S. Department of Health and Human Services, which oversees Medicare. "He said to me, 'Hey, I don't know what your schedule is like, but maybe you could drive by this pharmacy in Hialeah; it's pretty hot,'" Hill recalls. The informant was an employee at a private company reviewing Medicare claims. So Hill, a former Jackson County, Missouri, sheriff's deputy

who had once worked on a drug task force, decided to check things out. Surveillance work is second nature to him. But he admits that such jobs can be numbing, particularly in the subtropics where the sun can tire the eyes and the humid heat can scramble the focus that's necessary. On a stakeout, no matter how monotonous things get, you can't afford to be distracted. Glance away and you might miss someone walking out a door or driving slowly by in a car.

The "quick hit" on Elbia's Pharmacy shows there may be a way to stanch the flow of taxpayer dollars lost to fraud.

For an entire day, Hill and his partner sat staring at the Elbia's Pharmacy building. Nobody went in; nobody went out. The lights never flickered on.

At the same time that Hill was staring at Elbia's closed doors, the OIG was monitoring the pharmacy's online billing activity. Sure enough, during the same day--April 7, 2010--Elbia's billed Medicare around $100,000 for high-priced prescription drugs such as Zyprexa, Lovenox, and Risperdal. By contrast, the previous owner billed Medicare about $1,000 a week. It was as close to a real-time investigation of a crime as you can get--like watching thieves drilling through a bank's vault.

On the second day of the stakeout, at about 10:30 a.m., Hill and his partner noticed that a man approached Elbia's and opened the door. Not so many years back, the agents might have taken his photo and waited. But there is a sense of urgency about this crime now. The longer they wait, the more money is lost. So the agents jumped at their chance, rushing over from their car to confront the guy, a chubby Latino with a double chin. "We asked what he was doing and he said he was picking up the mail," Hill recalls. The man explained how the owner of the pharmacy had hired him for $50 to pick up a UPS package. "Then we asked him who owned the place, and he said a man named Alberto." The agents told the courier they wanted to talk to Alberto, and the man dialed a number on his cell phone. When "Alberto" answered, the agents took the phone. "We said we'd like to meet him," Hill says. But Alberto said he was out of town. He would try to come in the next day.

The courier presented the two agents with a driver's license revealing his name to be Luis Perez Moreira. Hill asked if Moreira could show them around the shop. He agreed to take them inside. And at that point it became clear that whatever Elbia's may have once been, it was no longer a pharmacy in any conventional sense. There was no inventory or pharmacist. There were no customers. "The walls were bare," Hill says. As soon as the agents took a look at the interior, they called the U.S. Attorney's Office to ask prosecutor H. Ron Davidson to help issue a search warrant. An hour and a half later, warrant in hand, the agents returned to Elbia's to conduct a search. But there was nothing to find.

There is health-care fraud all over the country, to be sure, but in the region of South Florida comprising Miami-Dade, Broward, and Palm Beach counties, it is in an advanced state. Here, it is fueled by large populations of the elderly, who are enrolled in Medicare; and by poor immigrants, who because of economic desperation or language barriers can be easily manipulated by criminals. This area has the densest concentration of Medicare providers in the country, with one for every 500 Medicare beneficiaries. In contrast, the rest of the country averages about one provider for every 3,000 beneficiaries. To judge by the medical data, you would think South Florida was made up entirely of the sick, the limbless, the crazy. And in this sense, South Florida is both an illustration of the Medicare fraud problem and its bellwether. If the fraud here can't be contained, it does not bode well for the rest of the country.

Over the past decade, individual criminal rings in South Florida have netted hundreds of millions of dollars at a time. This is drug-cartel level profit, but without the gunfights. And it has spawned a supporting economy to service it. There is a brisk trade in stolen patient and doctor IDs. Shady car

dealerships and check-cashing stores provide fronts for money laundering. Disreputable lawyers reportedly hold seminars on how to set up shop and bill the government. One former prosecutor I talked with speculated that Miami's economy would grind to a halt if all Medicare fraud stopped overnight. In certain parts of town, it is easy to find low-rent office complexes packed with doctors' offices, therapy clinics, and medical-supply stores all closed in the middle of the day. Many of the ones that are open have the exact same sign posted by the door: *please be advised that this office will not allow unannounced visits by insurance company investigators.* "It is an epidemic, and it is viral," says Wifredo Ferrer, the U.S. attorney for the Southern District of Florida, who has made Medicare fraud one of his office's top priorities since taking the job in 2010.

The Centers for Medicare and Medicaid Services (CMS) spent more than $500 billion last year on Medicare's free and reduced-cost medical service for people aged 65 and over and those who qualify for disability under Social Security. But CMS has also been a thieves' piñata for more than a decade. What happened at Elbia's Pharmacy suggests there may be ways to stanch the flow of billions of taxpayer dollars lost each year to fraud: Law enforcement now has the ability to monitor, in real time, the sprawling computer networks that handle the patient, medical service, and payment information for one of the U.S. government's largest annual expenditures. What seems equally true, though, is that the scale of the Medicare problem may be beyond the modest scope of our current efforts to combat it. Indeed, without the kind of modern tools that credit-card companies and online retailers use to prevent fraud, it may be impossible.

The number repeated by most government agencies is that about 10% of CMS's expenditures are lost through fraud and "improper payments." The Government Accountability Office (GAO), the investigative arm of Congress, repeatedly labels Medicare and Medicaid "high-risk programs" because their size and complexity make them so vulnerable to fraud, waste, and abuse. CMS itself estimates that in 2010 it made a total of more than $48 billion in improper payments in Medicare, and another $22 billion in Medicaid. That's about 10% of the program's annual spending. (The FBI regularly estimates Medicare and Medicaid fraud at between 3% and 10%.) It's hard to imagine any private business enduring long-term fraud losses at that level.

Yet it may be far worse than that. Malcolm Sparrow, perhaps the leading academic on health-care fraud, says CMS estimates are almost certainly wrong. "The history of the 10% figure is that it came from a GAO report from the mid-1990s," Sparrow, the chair of the executive program on regulation and enforcement at Harvard's John F. Kennedy School of Government, explains. "If you track it down--and I did--it says in that GAO report that 'some industry experts believe the loss rate could be 10%.' And because that appeared in a government report, even in an extremely vague form, it was enough to justify using it." The figure stuck because it was convenient, Sparrow surmises. "Ten percent I think served the political purpose for a good long time," he says. It was big enough so that it didn't look like people were in denial, but "not so huge as to be a public embarrassment."

Sparrow, for one, has no doubt the figure is higher. He just doesn't know by how much. "We don't know, because they [CMS] have for years persistently failed to conduct rigorous measurement studies to produce valid estimates," he says. In the 1990s, Clinton administration officials urged Sparrow, a former chief inspector with the British Police Service, to study fraud control within the health-care industry. He found that bureaucracies were good at making sure claims were processed correctly, but not good at ferreting out fraudulent claims. The analysis still holds true today, he contends. After Congress passed a 2002 law forcing all major government programs to evaluate their error rates, Sparrow examined CMS's audit methods. There were no on-site audits of Medicare providers, and in most cases, the studies did not involve any contact with patients. As Sparrow sees it, criminals have learned that if they lie twice, once when they submit a claim and once when they

submit supporting medical documentation, they can escape detection. "The rule for criminals is simple," Sparrow testified before a Senate subcommittee on crime and drugs in 2009. "If you want to steal from Medicare or Medicaid, or any other health-care-insurance program, learn to bill your lies correctly."

What may at first seem like an accounting disagreement at a big government agency actually has profound implications for U.S. policy and society. Congress is presently mired in an endless debate about when--and how much--to cut entitlement programs in an effort to reduce the federal deficit. The Obama administration proposes trimming $248 billion over 10 years from Medicare alone. Yet if fraudulent losses could be reduced by just a few percentage points, the issue becomes moot--and the medical support that tens of millions of Americans rely upon could continue uninterrupted. "The annual combined cost of Medicare and Medicaid is between $800 and $900 billion annually," Sparrow says. If only 10% is lost to fraud, he notes, that's $80 billion a year--pointing to a figure even higher than the $70 billion cited by the GAO. "But if it's 20% or 30%?" he asks. "We'd easily find $200 billion over 10 years. That means you wouldn't need to cut reimbursement rates for providers. You wouldn't need to restrict insurance coverage. You wouldn't have to increase deductibles. Getting hold of this problem is a much healthier way of dealing with the cost- control imperative than through indiscriminate cutbacks." The question thus becomes whether the politicians in Washington who are now trying to cut spending on medical care are actually wrestling with the wrong problem. Which means they might settle on the wrong solution.

In contrast to Medicare, which suffers fraud losses of at least 10%, credit-card companies lose less than 1%.

Criminals have almost certainly been stealing from Medicare since the moment Lyndon B. Johnson first signed the program into law in 1965. Miami prosecutors recall with nostalgia the "Medicare milk" scams of the 1980s, in which doctors wrote prescriptions for unnecessary liquid nutrition that was then sold on the black market. These were followed by something known as "up-coding" scandals (where clinics billed for more expensive procedures than were performed) and fake equipment rentals (in which stores billed Medicare for unnecessary hospital beds and wheelchairs). But at least in those cases, there were actual wheelchairs and beds. There were actual doctors and patients.

With the advent of identity theft and the proliferation of electronic transactions, all that has become unnecessary; in many cases, all you need to run a Medicare scam is a basic knowledge of the billing process and a post-office box to collect the checks. Nowadays, criminals create fake clinics or stores, much like Elbia's Pharmacy, and bill Medicare with phantom patients along with the unique NPI (national provider identifier) of doctors who are supposedly treating them. Often, this information--especially the IDs and Social Security numbers of phantom patients--is provided to the fake clinic or store by corrupt hospital and insurance-company employees.

"It started to really take off in the early to mid-2000s," says Ferrer, South Florida's current U.S. attorney. "That's when we saw the uptick." That also seems to be when the feds began paying closer attention. In 2005, R. Alexander Acosta, Ferrer's predecessor, created teams of FBI agents and OIG investigators to focus solely on health-care fraud. The teams were set up like drug squads, geared to catch fraudsters in the act and take them down quickly with the proceeds they had on them. "We called them 'quick-hit squads,'" Acosta recalls. "Our goal was to get them in the act and prosecute them for what we caught them with." The priority had shifted to protecting the money, but it was slow-going getting the data they needed from CMS. "Up until then, we had to refer a case to CMS and have them look at the billing," Acosta says. Waiting for a response was

frustrating. "It would take 90 days to get the information we wanted," says Gary Cantrell, assistant inspector general for investigations at the OIG's headquarters, in D.C.

So the investigators invited CMS to partner with them. CMS gave agents access to its computer system and provided real-time access to the network. This was the boost they needed. The feds used a nurse-practitioner and an analyst to comb through data and catch anomalies, such as female patients receiving penis pumps (which are, indeed, reimbursable), or alleged amputees receiving prostheses for all four limbs, as well as spikes in bills for certain drugs. These "quick-hit" teams in South Florida were successful enough that the Department of Justice copied the model nationally in 2007. (In 2010, a total of 192 defendants were charged with trying to defraud Medicare out of $417 million.)

The crackdown on Elbia's is a typical example of how these efforts work. On April 9, the day after agents searched the pharmacy, and two days after Agent Hill first staked out the place, the business was officially closed down. Agents had already contacted at least three people whose identities were used to bill Medicare, and all said they had never heard of the pharmacy. One doctor discovered that Elbia's had billed $110,000 in drugs using his name. Open nine days under its new owners, Elbia's had billed Medicare for $776,298 worth of drugs. But thanks to the quick-hit approach, the pharmacy received a grand total of just $70 in payments.

Still, the fraud has outpaced these efforts to combat it. For instance, in 2006, Miami's OIG office sent agents to audit more than 1,500 medical-equipment providers registered with Medicare in South Florida. It was an effort to gather basic information. But it had the effect of exposing the sheer pervasiveness of the problem. Agents found that one in three providers had no legitimate address, was located in an empty office, or was closed during weekday work hours on repeated visits. In 2009, Ferrer says, when home-health care fraud exploded, bills for nursing visits in Miami -Dade County exceeded the combined totals in Atlanta, Chicago, and Dallas. Last year, he adds, Medicare claims from Miami-Dade County alone totaled $558 million, more than the combined total of 23 states. More alarming, there seems to be growing evidence that Florida-style fraud is spreading to other states. Within the past two years, federal strike forces have broken up fraud rings in Atlanta, Detroit, Los Angeles, and New Orleans. In the course of those busts, they've discovered the perpetrators usually hail from Miami, or that the schemes were hatched there.

At the very least, the approach that the OIG and U.S. prosecutors used to shut down Elbia's Pharmacy demonstrates the value in having investigators work closely with data analysts in deciding when and how to move in on a criminal enterprise. "Swiftly enough to chop the money flow," Harvard's Sparrow says. "But decisively enough to make sure bad players can't simply come around again under another guise." For this approach to have a systemwide impact, though, it would have to be stepped up as well as vastly expanded. As Sparrow envisions it, the antifraud efforts should start as soon as the claims come in. It would involve a random selection of claims for verification and employ a "veritable army of analysts," he says, to identify newly emerging fraud patterns.

All this would require a big investment from Washington--bigger than the $350 million Obama has added in his health-care plan to the government's customary antifraud funding. But the payback would almost certainly make it worthwhile. "Right now, overall spending on program integrity at CMS is hovering at 0.2% of spending. It used to be closer to 0.1%," Sparrow says. "However, you're looking at a problem where the loss could be 10% or it could be 30%. We don't know because there is no valid way of measuring it. The question is, Why aren't you doing 10 times as much?" Economists would say the optimal investment in loss control is the level at which a dollar spent produces roughly one dollar saved. "If you're spending a dollar and you are recovering $7, or

$17, you should keep spending until you get much closer to a one-to-one return ratio at the margin," Sparrow asserts.

Others who have worked the front lines point to obvious technical reforms that CMS could implement to deter theft. "When you retire and go on Medicare, do you know what your Medicare number is?" Acosta, the former U.S. attorney in Miami, asks. "It's your Social Security number. CMS doesn't have a way to provide personally unique numbers. Anyone with your Social Security number can bill on your behalf. It's as if you told American Express that your card had been stolen, and they issued you a new card with the same number on it and told you they'd monitor it. That doesn't make a lot of sense to me." To illustrate how things could work, Acosta recounts how four days after Hurricane Katrina, PayPal, the online money-transaction service, contacted authorities in Miami. PayPal had noticed a spike in funds going to a local outfit taking donations to airlift supplies into the New Orleans airport. "Well, the New Orleans airport was closed," Acosta says, so authorities were able to quickly shut down the operation. "CMS doesn't have that kind of capability."

The analog to the credit-card industry is one that many experts make. Credit-card companies boast a fraud loss rate hovering around 1%, according to Ben Woolsey, a former financial analyst in the credit-card industry and now the marketing director for the consumer resource website CreditCards.com. A loss rate of 10%, which is the accepted number for CMS, would drive credit-card companies out of business. "They really couldn't survive if losses were that high," Woolsey says. "The reason that fraud stays relatively low is that the card industry has very sophisticated methods for recognizing fraudulent activity. Since it's their money being spent they have the ability to shut down the account if they suspect anything is out of order." The companies have honed their computer systems to develop pattern-recognition programs using the vast database of customer transactions. Over time, Woolsey says, neural networks can learn to recognize statistical patterns within a given portfolio and detect suspicious activity. Anyone whose credit-card company has called to ask if they purchased surfboards in Australia can attest to this. It would seem obvious for CMS to mimic the credit-card industry in this regard.

There are signs CMS understands the potential here. Right now, the agency is running a pilot project in Indianapolis, where Castlestone Advisors is providing cards to certain Medicare vendors and doctors. The card must be swiped at a local doctor's office to initiate a transaction for durable medical equipment (DME), thus creating a time, date, and place log for an order. If you're in Miami when you swipe that card, CMS will know something's amiss. All the claims that these DME suppliers submit to Medicare can be verified this way. The company's founder, Jeff Leston, envisions using space on existing credit-card networks and deploying the cards universally through the Medicare system.

It turned out that the mysterious owner of Elbia's Pharmacy known as Alberto never showed up for his appointment with Agent Hill. In fact, the job of finding out who was behind the scam was not nearly as easy as turning off the spigot of money. The man registered with the state's division of corporations as Elbia's owner, Emilio Tain, was quickly found and brought in. Confronted with the evidence, Tain agreed to cooperate. The problem was that Tain was little more than a fall guy paid to put his name on some paperwork. He only knew the two men who hired him by their aliases--Alberto Fernandez and his partner, Moises. Tain did offer one piece of evidence: a photo he had taken with his cell-phone camera of one of the men's cars, a silver Mercedes SL. The license plate was clearly visible. He gave that photo to the feds.

When the name on the Mercedes registration turned into a dead-end, investigators ran the license plate to see if the car had any tickets or been involved in any accidents. And sure enough, Hialeah

police had written a traffic ticket for that Mercedes recently. It was issued to a 28-year-old Cuban native named Sarody Milian. Agents pulled his driver's license photo and showed it to Tain, who confirmed that it was Alberto Fernandez. Not long after, the agents pulled surveillance footage of Milian making deposits at banks where Elbia's had accounts and showed it to the woman who had sold the clinic, Elbia Doval, who also recognized him as Alberto Fernandez.

Meanwhile, the other partner in the scam--the man known as Moises--remained a mystery. That is, until agents pulled the driver's license photo of the only other person even remotely connected to the case, the courier they met at Elbia's, Luis Perez Moreira. Both Tain and Doval identified him as Milian's partner "Moises."

Both men turned out to be veteran fraudsters. Milian was already facing state charges for staging auto accidents in an insurance scam. Moreira was a suspect in another health-care-fraud crime, also involving a fake clinic, where CMS had allegedly paid him nearly $400,000. It took the feds until October 2010 to identify and locate Milian. Once he was in custody he eventually pleaded guilty. Moreira, meanwhile, remained a ghost.

On March 15, 2011, Milian walked into U.S. District Court Judge Paul Huck's courtroom in downtown Miami dressed in a drab khaki prison uniform with his hands shackled to his waist. He radiated youthfulness, with close-cut dark hair, acne on his cheeks, and an athletic frame. As he sat down next to his lawyer, Milian donned a pair of headphones so he could hear a translation of the proceeding. When Judge Huck asked if he had anything to say, Milian stood up and spoke in Spanish. "I would like to apologize to all the people in the court. This is all results of mistakes I made," he said. "It will never happen again." For emphasis he added, *"Nunca, nunca, nunca!"* (Never, never, never.)

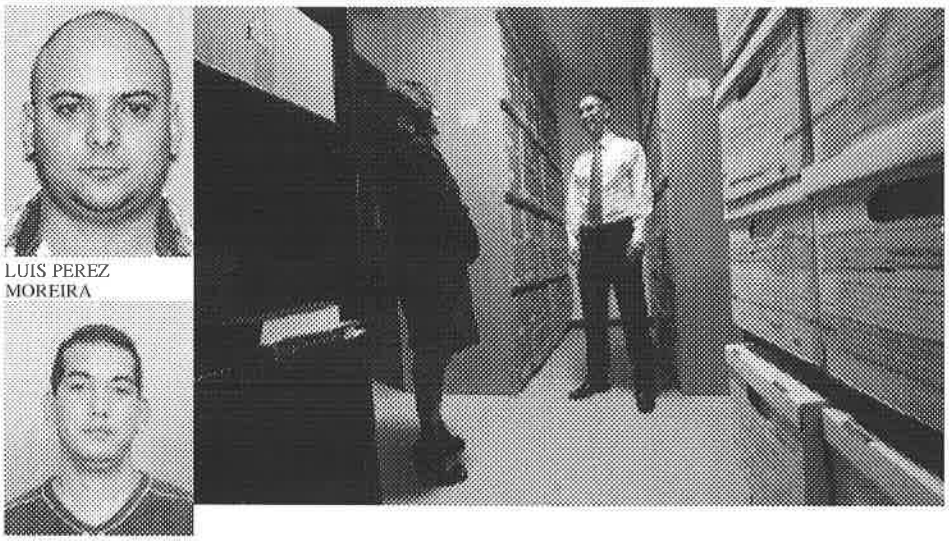
But Judge Huck's patience had worn thin at these sentencings. "I'm a little confused," he said. "What mistakes are you talking about?"

Milian looked up, his eyes wide. "Allowing myself to be used by another person," he offered. Huck glared at the defendant. "It bothers me when people say 'mistake.' It's not a mistake. It's a crime. You're a criminal." He paused. "I do not accept your statement. It's not a mistake."

Huck then made clear what he thought of the bureaucracy that has long been so thoroughly exploited by criminals. "It's encouraging to see that Medicare didn't pay," he mused as he glanced down at the paperwork before him. "Turns out the red flags went up so much so that *even* Medicare caught it." Milian and Moreira had "only billed three-quarters of a million dollars," Huck said, before catching himself. "Saying 'only three-quarters of a million' sounds kind of odd, doesn't it?" he told the courtroom. But in Miami it's the everyday truth.

Postscript: Milian was sentenced to 33 months in prison and ordered to pay back $70 for the Elbia's Pharmacy fraud. Less than three months later, TSA officials grabbed Moreira as he arrived at Miami International Airport. He pleaded guilty this summer and was sentenced to five years and three months in prison and ordered to pay back $380,000 for a previous fraud.

A Strike Force Hit



LUIS PEREZ MOREIRA

SARODY MILIAN

H. Ron Davidson (above), the U.S. prosecutor in Florida who oversaw the rapid response effort to shut down Elbia's Pharmacy. The strike netted two veteran fraudsters: Milian was already facing charges for insurance scams; Moreira was a suspect in another fake medical-clinic investigation.

A version of this article appears in the December 2011/January 2012 issue of Fast Company.

Links:
[1] http://www.fastcompany.com/magazine/161/how-to-commit-medicare-fraud-in-six-easy-steps