GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Office of Special Investigations

B-283695

October 5, 1999

The Honorable Susan M. Collins
Chairman
Permanent Subcommittee on
Investigations
Committee on Governmental Affairs
United States Senate

Subject: Health Care: Fraud Schemes Committed by Career Criminals and Organized Criminal Groups and Impact on Consumers and Legitimate Health Care Providers

Dear Madam Chairman:

This report responds to your July 27, 1998, request that we provide you with information concerning the nature and magnitude of illegal activity by career criminal and organized criminal groups posing as health care providers for the purpose of defrauding federal, state, and private insurance systems. Both Medicare and Medicaid programs, because of their size and complexity, are vulnerable to fraud and abuse. We have reported previously about the importance of controlling health care costs, especially in the federal government.[1] Controlling fraud is part of the remedy for controlling health care costs. In fiscal year 1998, the latest year for which statistics are available, Medicare paid out more than $193 billion and Medicaid spent approximately $177 billion.

The Coalition Against Insurance Fraud, using private insurance information provided by the Health Insurance Association of America and public insurance information supplied by the Health Care Financing Administration (HCFA), estimated the dollar amount of nationwide health care claim fraud for 1997[2] to be $53.9 billion. Of this amount, approximately $20 billion was attributed to fraudulent private insurance claims; and approximately $34 billion was attributed to fraudulent public insurance claims, including Medicare and

[1] *Medicare: HCFA's Use of Anti-Fraud-and-Abuse Funding and Authorities* (GAO/HEHS-98-160, June 1, 1998*); Private Health Insurance: Continued Erosion of Coverage Linked to Cost Pressures* (GAO/HEHS-97-122, July 24, 1997); *Medicaid Fraud and Abuse: Stronger Action Needed to Remove Excluded Providers From Federal Health Programs* (GAO/HEHS-97-63, Mar. 31, 1997); *High Risk Series: Medicare* (GAO/HR-97-10, Feb. 1997).

[2] The most current year for which statistics were available was 1997.

Medicaid.[3] There is a growing trend in health care fraud in which sham providers are entering the health care system with the sole and explicit purpose of exploiting it. Rather than first providing services at an inflated cost, these criminals often bill Medicare while providing no or inferior services. As our review determined, however, this trend is not limited to the Medicare program. State Medicaid programs and private insurers throughout the country are being defrauded in the same manner. Within the past several years, state and federal law enforcement officials in every part of the country have uncovered such fraud.

In order to address the proliferation of health care fraud on the part of criminals and organized criminal groups, you asked us to report on (1) the makeup and prior activities of such groups; (2) how organized criminal groups created medical entities or used legitimate medical entities or individuals to defraud Medicare, Medicaid, and private insurers; (3) schemes used by such groups to commit health care fraud; and (4) the impact that illegal activity by such groups has on consumers and legitimate health care providers.

To develop this information, we identified seven criminal health care fraud investigations for review. In the four cases involving Medicare and Medicaid fraud, the leaders of each criminal group pled guilty to federal or state criminal charges related to health care fraud. These charges included conspiracy to defraud the United States, conspiracy to commit money laundering, mail fraud, racketeering, conspiracy to commit racketeering, and/or organized fraud. In the three private insurance cases, the leaders of each group were indicted: one is awaiting trial while the other two are fugitives. Cases against other group members in each of the seven groups are in various stages of completion, with some members having pled guilty to criminal charges and other members in fugitive status following indictments.

We interviewed federal and state law enforcement officials associated with the investigations we reviewed and largely relied upon their investigative findings in preparing our report. Plea agreements, along with stipulations of fact and/or criminal information contained in court documents, generally confirmed many of the investigative findings. The investigations involved criminal groups that were representing themselves as legitimate providers and, allegedly, billing public and private insurance systems for medical services and equipment not rendered or not necessary. The cases we reviewed involved a combination of Medicare, Medicaid, and private insurance fraud or alleged fraud occurring in Florida, North Carolina, and Illinois between 1992 and 1998, with the period of fraud or alleged fraud in each case lasting between 3 months and 4 years. In the seven cases we reviewed, the fraudulent claims ranged from between $795,000 to more than $120 million, of which between $72,000 and over $32 million were actually paid by either Medicare, Medicaid, private insurers, or a combination thereof. With respect to the cases involving private insurers, alleged fraudulent claims were filed with between 18 to over 100 insurance companies and self-insured plans. (See encl. I for a more detailed scope and methodology.)

[3] These figures are estimates of claim fraud. They do not include costs related to the detection, investigation, or prosecution of insurance fraud, nor has there been any attempt to estimate the amount of fraud committed by insurers or those purported to be in the business of insurance.

Results in Brief

While the full extent of the problem remains unknown, we did determine that career criminal and organized criminal groups are involved in Medicare, Medicaid, and private insurance health care fraud or alleged fraud throughout the country. In the cases we reviewed, criminal groups varied in size from 2 or 3 participants to more than 20 participants and generally had one leader. Many group members had prior criminal histories for criminal activity unrelated to health care fraud, indicating that they moved from one field of criminal activity to another. The primary subjects in these cases had little or no known medical or health care education, training, or experience. At least two groups learned or were suspected of having learned how to commit health care fraud from others already engaged in such fraud. In some of the cases we reviewed, criminal-group members had relatives or associates in foreign countries who helped them transfer their ill-gotten health care proceeds.

These groups created as many as 160 sham medical entities—such as medical clinics, physician groups, diagnostic laboratories, and durable medical equipment (DME)[4] companies, often using fictitious names or the names of others on paperwork—or used the names of uninvolved legitimate providers to bill for services and equipment not provided or not medically necessary. For the most part, these entities existed only on paper. Once the structure was in place, subjects used a variety of schemes to submit claims to Medicare, Medicaid, or private insurance companies.

One scheme used is sometimes referred to as "patient brokering" or "rent-a-patient." Under this scheme, which was used in one of the Medicare cases, the subjects used "recruiters"[5] (also known as "runners") to organize and recruit beneficiaries (patients)[6] who visited clinics owned or operated by such subjects for unnecessary diagnostic testing and/or medical services. Recruiters received a fee for each beneficiary brought in; hence they "rented" or "brokered" the beneficiary and/or identifying information to the subjects. In turn, recruiters paid a portion of their fee to each cooperating beneficiary. The beneficiaries' insurance was later billed for these and other services or equipment not provided. In addition to the beneficiaries, some physicians were willing to collaborate with subjects in exchange for money.

Another successful scheme is commonly referred to as "drop box" or "mail drop." In this scheme, which was used in six of the seven cases[7] according to investigators, subjects rented

---

[4] Durable medical equipment, or "DME," includes such things as iron lungs, oxygen tents, oxygen concentrators, hospital beds, and wheelchairs used in the patient's home, whether furnished on a rental basis or purchased; blood-testing strips and blood glucose monitors for individuals with diabetes; and seat-lifting mechanisms.

[5] "Recruiters" are individuals who are paid by providers to bring beneficiaries to their clinics or offices for unnecessary medical services at no charge to the beneficiaries. Recruiters usually share a portion of their fees with cooperating beneficiaries.

[6] Medicare-covered patients are most often referred to as "beneficiaries"; Medicaid-covered patients are referred to as "recipients"; and private insurance-covered patients are referred to as "insureds." For the purpose of simplification, we will refer to all insured individuals (patients) as "beneficiaries" in this report.

[7] In the seventh case, the basic elements of the drop box scheme were used without the use of private mailboxes. In that case, the subject received fraudulent medical payments electronically.

private mailboxes or drop boxes, set up bogus corporations, and opened phony corporate bank accounts. Subjects then used stolen, purchased, or otherwise obtained beneficiary and provider information to bill insurance plans for medical services and equipment not provided. Members of the criminal groups retrieved insurance checks from the drop boxes and deposited them into controlled bank accounts. Once deposited, proceeds were quickly converted to cash or transferred to other accounts and moved out of the reach of authorities. These activities sometimes continued even after subjects were indicted, arrested, or jailed.

The above-described activities affect consumers, beneficiaries, health care providers, and law enforcement officials. Consumers pay increased health care costs in the form of taxes, because taxpayer contributions support Medicare and Medicaid. In the case of private insurance, insured individuals pay increased premiums. According to investigators and doctors, false medical histories for some beneficiaries could affect the care prescribed, as the care could be based on false data. Beneficiaries also unknowingly risk exhaustion of their insurance benefits, due to false information included in the claims that use their names. Legitimate providers may find their reputations tarnished and their provider numbers suspended when investigators look into alleged fraud committed in the names of these legitimate providers. Such inquiry may also delay payment of their legitimate claims. Because of the multiplicity of schemes and the ease with which subjects move their operations from location to location, law enforcement officials find it difficult to keep up with this growing and widespread form of fraud and are often unable to seize or recoup fraudulent proceeds that are quickly moved out of their reach.

Criminals and Other Individuals With No Known Prior Criminal History Have Migrated to the Health Care Field

Criminals previously involved in other types of crime are now migrating into the health care fraud arena. In at least four of the seven cases we reviewed, some of the subjects had prior criminal records for crimes unrelated to health care, including securities fraud, narcotics violations, tax evasion, weapons violations, forgery, grand theft auto, and criminal boating violations. In one case, two of the subjects were on probation for non-health-care-related crimes at the time they committed the health care fraud. In three cases where there were no known prior criminal records, the individuals had connections to other criminal groups or individuals reportedly involved in health care fraud.

In the Illinois Medicaid case, an individual in New Jersey sent four individuals to Illinois to open a laboratory. When the group arrived in Illinois and purchased a lab, the previous lab owner had to teach them how to operate the lab and how to bill Medicaid and Medicare because the four had no prior experience operating medical laboratories. The group purportedly cashed the Medicaid insurance checks it received and forwarded them to the New Jersey individual. The investigator later found out that the New Jersey individual was under investigation for health care fraud.

We found other cases in which health care criminal groups were teaching health care fraud to others and expanding into other geographical areas. In the North Carolina Medicare case, three subjects residing in North Carolina traveled to Florida where relatives taught them how to anonymously file false Medicare claims. They then returned to North Carolina and began

filing such claims. In one of the Florida private insurance cases, the investigator suspected the subject had learned how to commit health care fraud from two former employers who had previously been investigated for Medicaid fraud in South Florida.

In the cases we reviewed, according to investigators, the leaders of the groups had little or no known medical or health care education, training, or experience; and none possessed medical licenses.

Some of the individuals involved with the criminal groups investigated used relatives and associates in other countries to help them transfer fraudulently obtained money.

Criminal Groups Created Sham Medical Entities or Used Legitimate Medical Entities to Defraud Public and Private Health Insurance Systems

In six of the seven cases we reviewed, individuals in the criminal groups incorporated or otherwise set up as many as 160 medical clinics, physician groups, diagnostic labs, and/or DME companies to submit fraudulent or allegedly fraudulent public and/or private health insurance claims. In the seventh case, the subject used the names of four real clinics; but he changed their addresses on allegedly fraudulent claims so that payments would be mailed to private mailboxes that he controlled.

Typically, the leader of the group, in conjunction with others, would set up the medical facility by filing incorporation documents and obtaining state and federal certifications and provider numbers, where required, and, in some cases, taxpayer identification numbers (TIN). In two of the cases we reviewed, an actual physical location was set up for at least one of the companies established. For example, in the Illinois Medicaid case involving a laboratory, the subject paid 1 month's lease on office space and state-of-the-art medical testing equipment to obtain the certification needed to bill Medicaid for complex lab tests. Afterward, no patients were ever seen in the lab. In the Florida Medicare case, some clinics were opened to perform unnecessary diagnostic procedures on cooperating beneficiaries.

In most cases, however, the medical entities existed only on paper. To maintain anonymity, leaders of the groups frequently set up medical entities using fictitious names or the names of other group members, including relatives or associates. They sometimes fabricated identification cards by using their own picture but the name and identifying information of an uninvolved, unsuspecting individual. In one instance, the leader of the group opened companies in the names of individuals he met while serving time in prison. In the North Carolina Medicare case, the subjects searched for and found two individuals who wanted to leave the United States. The subjects paid each of the individuals $100,000 for the use of their identities to set up corporations, bank accounts, and mail boxes and to obtain TINs, Medicare supplier numbers, and local licenses. Both individuals later left the country.

Once the framework was in place, subjects in the cases we reviewed used a variety of schemes to file claims with Medicare, Medicaid, and/or private insurance plans for medical services and/or equipment not provided or not medically necessary.

Criminal Groups Collaborated With or Used Beneficiaries, Physicians, and Clinics to Commit Alleged Health Care Fraud

In a scheme sometimes referred to as "rent-a-patient," recruiters organized beneficiaries to go to subjects' clinics for unnecessary diagnostic testing and/or medical services. The beneficiaries' insurance was billed for those services and often for other services or medical equipment never provided. Licensed physicians sometimes participated in such schemes, typically exchanging their signatures on medical records for cash, without actually performing or overseeing any medical services, or providing Certificates of Medical Necessity (CMN)[8] for DME equipment not provided or necessary.

In addition to recruiting willing beneficiaries and providers, members of these criminal groups purchased, stole, or otherwise obtained beneficiary, physician, and clinic information to bill insurance plans for medical services or equipment never provided in another scheme, referred to as "drop box," because the groups used private mailboxes to effectuate the scheme. In some cases, subjects attached fictitious doctor names to claims.

Use of Recruiters and Cooperating Beneficiaries

In two of the South Florida cases we analyzed involving Medicare and Medicaid fraud, recruiters organized and recruited thousands of beneficiaries from, among other places, low-income housing projects and retirement communities and drove them to area clinics for rote examinations and unnecessary testing, treatment, or DME referrals. Recruiters, predominantly elderly women in one case, generally received a fee of $100 to $135 for each beneficiary they brought in. In turn, recruiters paid a portion of their fee to each cooperating beneficiary. Cooperating beneficiaries participated to "make a few bucks" and understood that if they needed "a real doctor," they were to go elsewhere.

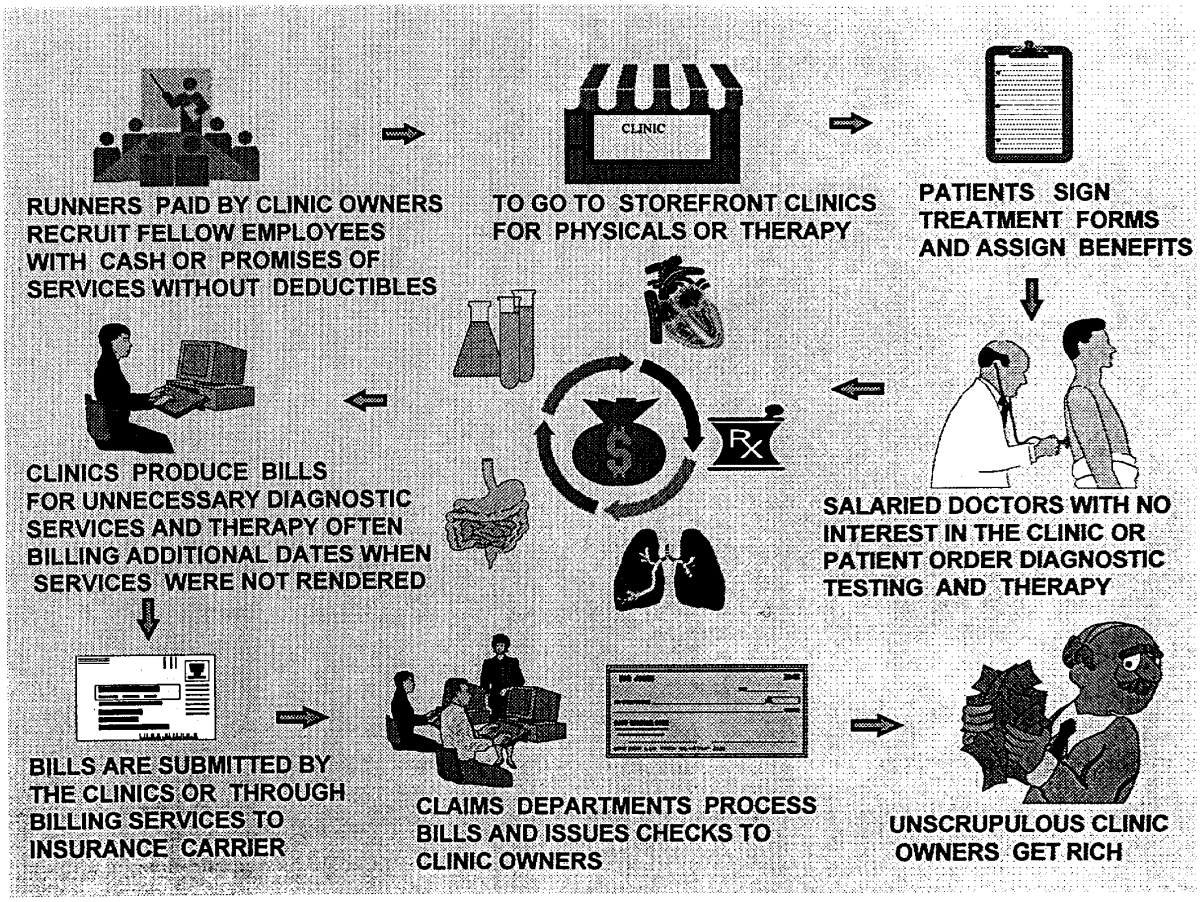
In some cases, according to law enforcement officials, cooperating beneficiaries were known to have been solicited to go to a private apartment to have x-rays taken via portable x-ray units or to have blood drawn. The beneficiaries received cash or unneeded prescriptions, which they later filled and sold on the street. Their insurance plans were billed for x-rays, blood tests, or other unnecessary services or equipment.

In some cases, beneficiaries have been known to provide only their insurance (i.e., Medicaid) number in exchange for cash. A laboratory would later bill their insurance for blood tests it conducted using someone else's blood. Also, clinic owners would send blood samples to labs

[8] A valid CMN is required for the payment of Medicare claims for DME. A valid CMN is one that the treating physician has attested to and signed, supporting the medical need for the DME item, and on which appropriate individuals have completed the medical portion.

to conduct tests and bill Medicare or Medicaid, and the labs would "kick back" some of the money to the clinic owners. An official from the New Jersey State Attorney General's Office, Medicaid Fraud Section, stated, "Most [beneficiaries] know that their Medicaid card is better than a VISA card for getting money." In essence, under this scheme, beneficiary and/or identifying information is "rented" or "brokered" to subjects. (See fig. 1.)

Figure 1: "Rent-a-Patient" Scheme



Source: Florida Department of Insurance, Division of Insurance Fraud

Use of Cooperating Physicians and Physician Assistants

In two South Florida cases involving Medicare and Medicaid, some licensed medical doctors and several foreign medical school graduates, some of whom were certified physician assistants, cooperated in the schemes. In the Florida Medicare case, which involved clinics and DME companies, the medical school graduates and/or physician assistants performed the actual procedures, including administering noninvasive medical tests and filling out medical charts. Licensed physicians were then paid $50 to $100 per medical chart to periodically sign medical records for services they neither performed nor supervised or to provide referrals or CMNs for DME that was not needed. (See also fig. 1.) Although they signed for services

purportedly performed by them or under their direction or observation, they were, in fact, not present when the services were performed.[9]

In the Florida Medicaid case involving DME companies, two clinic doctors were compensated for providing CMNs, which allowed the subjects to bill for unneeded oxygen concentrators through their DME companies.

Identities of Beneficiaries, Physicians, and Legitimate Clinics Used on Claims Without Their Authorization or Knowledge

Victim Beneficiaries

In all cases we reviewed, subjects used at least some "victim"[10] beneficiary information that was purchased, stolen, or otherwise obtained to file false Medicare, Medicaid, and/or private insurance claims. These victim beneficiaries received no medical services or supplies, were not involved in the fraudulent and alleged fraudulent activity, were not aware their names had been used on the claims, and did not authorize the use of their identities on such claims. According to law enforcement authorities, the identities of an estimated 35 to 2,500 victim beneficiaries were compromised in each of the seven cases. Some beneficiaries learned of the fraudulent and alleged fraudulent claims when they received Explanation of Benefits (EOB), Explanation of Medical Benefits (EOMB), or Medical Summary Notice (MSN)[11] forms in the mail from the relevant insurer showing services or equipment they did not receive. Others learned of the fraud and alleged fraud when their insurer notified them about questionable claims filed or investigators contacted them looking into such claims. In the Illinois Medicaid case and one of the Florida private insurance cases, claims were filed for more than 17 beneficiaries who had died prior to the purported dates of medical service as shown on such claims. The claims were not paid.

- In some of the cases we reviewed, investigators told us they were able to tie several victim beneficiaries to a common hospital where all the beneficiaries had previously been treated, suggesting that someone in the hospital released beneficiary information to criminals.

- Providers in Charlotte, North Carolina, submitted Medicare claims for supplies and equipment purportedly provided to beneficiaries residing in South Florida upon orders of Charlotte-area physicians. In that case, the group leader had paid a relative—a physician

[9] The Medicare Carrier's Manual, Title B3, Section 2050 requires that the physician be physically present on the premises during the time of medical service for the service to be covered by Medicare.

[10] In this letter, the terms "victim" beneficiaries, "victim" physicians, and "victim" clinics refer to uninvolved individuals or entities whose identities were used on fraudulent health care claims or other documents without their knowledge or authorization.

[11] The relevant payer sends EOBs, EOMBs, and MSNs to beneficiaries after a claim has been processed. Such statements list charges that have been billed to the insurer on the insured's behalf. Beneficiaries are encouraged to check such statements to be sure they were not billed for services, medical supplies, or equipment they did not receive.

at a Miami hospital—to obtain beneficiary lists from the Miami hospital. The relative was paid $5 to $7 per patient name.

- In the Illinois Medicaid case, the subjects fraudulently billed Medicaid using patient billing information they had legitimately obtained when they purchased a clinical laboratory from another individual.

- In the Florida Medicare case, an informant purchased copies of Medicare identification cards from a records clerk employed by legitimate doctors. The records clerk had first approached the informant about selling the identification cards when they became acquainted at a local bingo hall.

- During our review, a doctor in Miami, Florida, told us that his billing discs were stolen in an office burglary, while cash was left behind. The doctor told us that after the burglary, he received phone calls from patients about suspicious EOBs with his name attached to them for services he had not rendered. He further stated that other doctors in the same building and in another nearby professional building were burglarized in the same manner.

- In the Florida Medicaid case, the group leader's sister-in-law, who worked for a company that transported Medicaid patients, provided him with lists of beneficiary information.

In addition to the above examples, an investigator with a private insurance company told us that lists of beneficiary names and identifying information are known to have been sold illegally for $50,000. We were also told that beneficiary information is sometimes stolen from hospitals or providers, taken from trash bins, or obtained by computer hackers.

Victim Physicians and Clinics

In the same way that victim beneficiary information was used, victim provider information was also used in fraudulent health care claims. Victim physicians and clinics were not aware of the false claims; had not treated or referred the beneficiaries in question for the services or equipment shown; had not authorized the use of their identities; and, in many cases, did not even know the beneficiaries shown on the claims. Victim providers often became aware of such claims filed in their names when they received telephone calls from beneficiaries inquiring or complaining about EOBs they received showing medical services or equipment they had not received. In other cases, they learned about such claims only after being contacted by criminal investigators. In each of the 7 cases we reviewed, subjects used the names and identifying information of between 2 and more than 120 victim physicians as either the providing physician or the referring physician on the claims they submitted and on CMNs.

- In one of the Florida private insurance cases, the leader of the group allegedly used the names of four legitimate clinics as the providers of service on insurance claims. He simply changed the addresses of the clinics on the claim forms to a private mailbox he controlled.

- In a Florida private insurance case, the leader of the group allegedly used a victim doctor's name to file claims and to open a bank account the group leader controlled. To open the account, he presented the bank with a resident alien identification card bearing his photograph and the victim doctor's name; he also had a social security card bearing the victim doctor's name. Checks from this bank account were made payable to the leader of the group.

- In addition, in the case of one of the Florida private insurance investigations, victim doctors listed on claims as the "treating" physicians told investigators that they were not affiliated with the clinic or the physician group listed on such claims.

- Subjects sometimes obtained physician names and unique physician identification numbers (UPIN)[12] from unscrupulous hospital employees. In the North Carolina Medicare case, for example, a coconspirator who worked as an accounts receivable manager at a local hospital provided physician names and UPINs to the leader of the group. While executing a search warrant relative to the same investigation, investigating agents found a nationwide provider directory, which listed physician names and UPINs.

An investigator from the Florida Division of Insurance Fraud told us that physician names and UPINs are readily available and showed us a physician telephone directory known as "The Little Blue Book," which lists physician names, addresses, specialties, and UPINs by county. The back of the directory includes an order form and a listing of all counties for which the directory is available, including metropolitan areas in most states. The investigating agents in the North Carolina Medicare case learned that nationwide provider names and UPINs can also be found on the Internet.

Fictitious Doctor Names Used on Claims

In two of the Florida private insurance cases, the investigators told us that the subjects also used the names of fictitious doctors on the claims they submitted. According to the investigator in one of the cases, the designation "M.D." followed fabricated names shown as the providers of services/billing entities on claims. The investigator determined there was no record of medical licensure under those names in the state of Florida.

[12] Physicians and nonphysician providers who order or refer services, including lab work, for beneficiaries must submit their names and their UPINs on HCFA-1500 (Health Insurance Claim Form).

Criminal Groups Used Third-Party Billing Companies, Private Mailboxes, and Bank Accounts to Defraud Medicare, Medicaid, and Private Insurance

In at least three of the investigations we reviewed, subjects used third-party billing companies to file fraudulent claims and receive payment. In one case, a factoring company[13] was also used. Subjects sometimes defrauded more than one system. In six of the seven cases we reviewed, subjects used a "drop box" scheme, that is, they set up phony corporations, private mailboxes, and corporate accounts. Members of the criminal group would retrieve the insurance checks from the private mailboxes and deposit them into the bank accounts that they controlled. Once deposited, proceeds would quickly be converted to cash or moved to other accounts and moved out of the reach of authorities. Some of the subjects had associates or relatives who helped them transfer the ill-gotten proceeds. In the seventh case, subjects used the basic elements of the drop box scheme but received medical payments electronically rather than through the use of private mailboxes.

Submission of Claims

In the Florida Medicare case involving the use of clinics and recruited beneficiaries, the suspect's employees generated computerized Medicare claims using biographical data and the names of recruited beneficiaries. They then downloaded the information to tapes and delivered the tapes to a third-party billing company that entered the information into its own computer and sent it electronically to Medicare. Medicare generated a confirmation receipt that was forwarded to a factoring company, and the factoring company electronically advanced a predetermined percentage of the anticipated Medicare payment to the subject's bank account. The investigator on this case stated that although he believes the third-party billing company started out as a legitimate company, the owner began to understand that it was more profitable to bill nonlegitimate claims. He ignored questionable claims from the subject even when the third-party billing company's employees raised concerns about the same beneficiary names repeatedly showing up on claims.

The Florida Medicaid case involved the use of two third-party billing companies to submit fraudulent claims for DME, namely oxygen concentrators. Individuals known to the subject operated both third-party billing companies and were aware that the claims were fraudulent. One of the third-party billing companies filed claims for DME for the subject based solely on beneficiary names and Medicaid numbers without required CMNs. When investigators asked the owner of the third-party billing company to produce the CMNs, she contacted the primary subject who, along with his associates, created the required CMNs. These fabricated CMNs were turned over to investigators the following day. (Subjects in one of the Florida private insurance cases used the same third-party billing company to file claims.)

Other subjects prepared fraudulent paper claims without the use of third-party billing companies. In the North Carolina Medicare case, the leader of the group prepared Medicare claims and related documents. After investigators questioned him about his retrieval of Medicare payments from a private mailbox, he disassembled the typewriter he had used to prepare the claims and instructed his daughter to dispose of the pieces. Later, when he

[13] Factoring companies purchase the accounts receivable of a firm at a discount price, thereby providing the firm with immediate working capital.

thought he was no longer being closely scrutinized, he had his daughters and other neighborhood girls generate paper claims to private insurance plans from a home computer.

Billing of More Than One Insurance System

In at least three of the seven cases we reviewed, career and organized criminal groups defrauded more than one system (i.e., Medicare, Medicaid, or private insurance systems) simultaneously or moved from one system to another after they were caught in one area. For example, in the Florida Medicare case, subjects had filed in excess of $120 million in fraudulent Medicare claims and $1.5 million in fraudulent Medicaid claims. Because the investigator in the Medicare case had made a referral to Medicaid, Medicaid was able to stop the payment of the $1.5 million in fraudulent Medicaid claims filed by the group.

In the North Carolina Medicare case, the leader of the group fled the country after being questioned by investigators about fraudulent Medicare claim payments. He returned to the United States a few weeks later and began submitting fraudulent health care claims to private insurance systems. This subject later told investigators that it was easy to get money from Medicare. However, according to the same individual, getting money from private insurers was so easy, it was "like stealing candy."

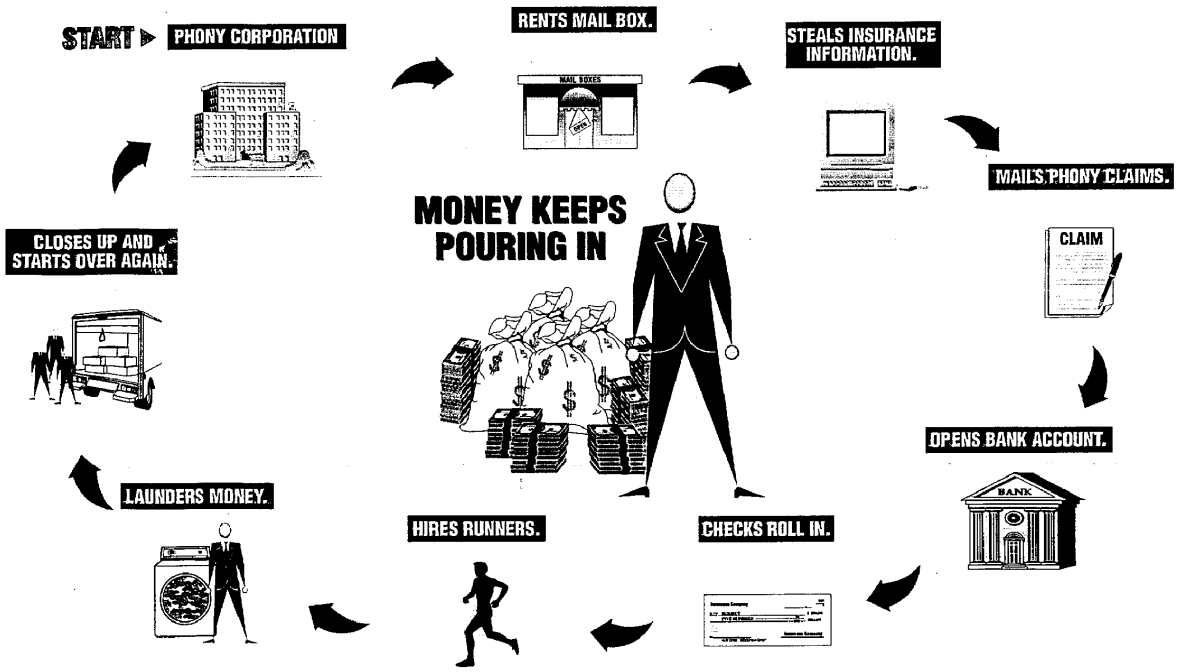
Use of Private Mailbox Facilities

To gain possession of insurance checks in payment of fraudulent health care claims, subjects in 6 of the 7 cases we reviewed had the checks sent to as many as 80 private mailboxes, or drop boxes. These mailboxes were opened at privately owned commercial mail receiving agencies (CMRA), including, among others, Mail Boxes Etc, A Mailbox for Less, and Pakmail Centers of America.[14] Fraudulent and allegedly fraudulent claims listed the addresses for providers/billing entities as the CMRA addresses, with the actual mailbox numbers generally appearing on claims as suite numbers, building numbers, or office numbers.[15] The group leader or other group members retrieved mail from these boxes. While some mail drop boxes were set up using the names of the group leader or cooperating coconspirators, others were set up using phony identification cards containing fictitious names or assumed identities along with photographs of the subjects. (See fig. 2.)

[14] There is no indication that these CMRAs were involved in the fraud, except for the North Carolina Medicare case. In that case, the subject purchased his own Mail Boxes Etc franchise and began using its mailboxes to further his fraudulent activity while also retaining mailboxes at other uninvolved franchises.

[15] A new CMRA regulation adopted by the U.S. Postal Service on Apr. 26, 1999, requires that all mail delivered to CMRAs be identified on its face as a private mailbox, or "PMB" (39 C.F.R. part 111 and *Domestic Mail Manual D042.2.6*). This regulation is meant to keep criminals from using CMRA addresses for credit card fraud and other scams. All CMRA customers must be in compliance by Apr. 26, 2000.

Figure 2: "Drop Box" Scheme



Source: Florida Department of Insurance, Division of Insurance Fraud

In one of the Florida private insurance cases where subjects operated within the Miami/Dade County area, 7 of 10 mail drop boxes were set up in other counties. The leader of the group paid the owners of the CMRAs in those locations to forward incoming mail, including checks representing payment of alleged fraudulent claims, to Miami/Dade County area mail drop boxes. The investigator explained that insurance companies know Miami is a "hot spot" for health care fraud activity and are less suspicious of claim payments going to addresses outside the Miami area. Mail drop boxes in other states were also tied to this group.

Use of Corporate Bank Accounts and Individuals to Transfer Money

In the cases we reviewed, fraudulently obtained funds were transferred in a variety of ways. Checks received at mail drop box locations and funds received electronically through billing companies were deposited into bank accounts that had been set up in (1) the names of the corporations, the subjects, the associates, or coconspirators or (2) fictitious or assumed names. Subjects then moved the money by cashing the insurance checks, writing checks to cash or individuals from bank accounts where insurance checks were deposited, and transferring funds between various corporate and individual bank accounts. Subjects sometimes used family members, friends, or associates in other countries to help them transfer their proceeds. In one case, a factoring company deposited claim payments electronically into bank accounts controlled by the subjects. According to an official of the New Jersey State Attorney General's Office, Medicaid Fraud Section, money laundering is the end result of most health care scams. Law enforcement officials find that

assets are placed out of the government's reach before the fraud is discovered and documented and that money is sometimes moved out of the country.

In the North Carolina Medicare case, for example, the leader of the group opened corporate bank accounts in the names of two individuals to whom he had paid $100,000 apiece for the use of their identities. He then transferred funds between bank accounts, with the majority of funds ultimately negotiated in the form of business checks to fictitious individuals. He had the checks shipped in blocks to family members and friends in Mexico via Federal Express and cashed by accomplices at banks in Mexico, including a Casa de Cambia (money exchange) where bank representatives converted the checks to U.S. and Mexican traveler's checks for a 5- to 8-percent fee. After deducting 10 percent for themselves, the accomplices shipped the remainder of the traveler's checks to the subject in the United States via Federal Express. The traveler's checks were subsequently spent or deposited to business or personal bank accounts. According to investigators, one of the subject's relatives in Mexico had a friend who worked in a Mexican bank. The friend would cash checks regardless of whose name was on them. In the same case, some of the funds sent to Mexico were converted to jewelry that was brought to the United States and resold by the group leader from his home.

In the Florida Medicaid case, the leader of the group paid family members and friends, including some he met while serving time in prison, to cash checks for him. In two of the Florida private insurance fraud cases, the leaders of the groups opened bank accounts in the names of legitimate, uninvolved providers, including a physician and four medical clinics whose names were used on allegedly fraudulent claims.

In another Florida private insurance fraud case, subjects deposited insurance checks to approximately 40 corporate bank accounts and then wired the money to European locations, through investment accounts. In the same case, an insurance official stated that her insurance company received cancelled insurance checks that had been cashed at a bank in Europe.

One subject in the Florida Medicare case directed his wife to send $4.5 million overseas. The money was then transferred back into the United States through an alleged mortgage fraud scam involving politicians in Florida. Subjects in this case would not cooperate with government officials who were trying to determine the disposition and location of the ill-gotten proceeds.

Legal Actions Often Ineffective in Halting Fraud

Legal actions against suspects do not guarantee that the criminal activity will stop. An official of the New Jersey State Attorney General's Office, Medicaid Fraud Section, stated that organized criminal groups tend to be quite transient. He provided examples, unrelated to the seven cases we reviewed, that demonstrate this point. In one case, suspects fled to California and started new operations before they could be arrested for violations that had occurred in New Jersey. In other cases, his office closed down New Jersey clinics only to find out that the New York Medicaid Fraud Control Unit was investigating the same individuals for different schemes.

In the Florida Medicare case we reviewed, the subject conducted business from the federal detention center while awaiting sentencing by using the detention center's telephone system and personal identification numbers assigned to other inmates. From the phone, he directed his wife on how to run the health care fraud business in his absence.

In one of the Florida private insurance fraud cases, three indicted subjects are believed to have fled the country and are considered fugitives. Investigators received information, however, that indicates that this group continued to submit allegedly fraudulent medical insurance claims from Panama through a freight-forwarding company in Miami, Florida, which acts as a private mail facility and intermediary.

Impacts of Health Care Fraud Perpetrated by Career Criminal and Organized Criminal Groups

Consumers pay increased health care costs as a result of health care fraud. Taxpayer contributions support the Medicare and Medicaid programs, so all taxpayers are paying for fraudulent claims paid by these programs. Also, additional health care costs to private insurers are passed on to insured individuals through increased premiums. Finally, self-insured companies risk going out of business when their health care costs become overwhelming due to fraudulent claims filed.

Beneficiaries, whose names are used on fraudulent claims, acquire false medical histories and risk exhaustion of their insurance benefits. Legitimate providers, whose identities are used on fraudulent claims without their authorization, may experience a variety of problems, such as delays in the payment of their legitimate claims, the receipt of IRS Forms 1099 for income never received, suspension of their provider numbers, or unearned tarnished reputations. Law enforcement officials find it difficult to keep up with this growing and widespread form of fraud and are often unable to seize or recoup fraudulent proceeds that are quickly moved out of their reach.

- - - - -

As agreed with your office, unless you release its contents earlier, we plan no further distribution of this letter until 30 days after the letter's date. At that time, we will send copies of this letter to interested congressional committees and will make copies available to others on request. If you have questions concerning the report, please contact Assistant Director Stephen V. Iannucci at (202) 512-6722. Special Agent Mary Balberchak was a key contributor on this assignment.

Sincerely yours,

Robert H. Hast
Acting Assistant Comptroller General
for Special Investigations

Enclosure

Enclosure I

Scope and Methodology

During this review, we examined the details of seven investigations wherein criminal groups representing themselves as legitimate providers fraudulently billed public and private insurance systems for medical services and equipment not rendered or not medically necessary. The investigations concerned fraud or alleged fraud committed in Florida, North Carolina, and Illinois with, in some cases, ties to other states and included two cases primarily involving Medicare, two cases primarily involving Medicaid, and three cases primarily involving private insurance systems, with some of these cases involving both public and private insurance systems. We selected these cases because they involved fraud and alleged fraud encompassing public and private insurance, different parts of the country, and significant dollar amounts in terms of fraudulent and allegedly fraudulent claims filed and paid and the significant number of victim beneficiaries.

We also interviewed federal and state law enforcement officials from the Federal Bureau of Investigation; Internal Revenue Service; U.S. Postal Inspection Service; Florida Division of Insurance Fraud; Office of the Florida State Attorney General/Medicaid Fraud Control Unit; Office of the New Jersey Attorney General/Medicaid Fraud Section; and State of Illinois/Medicaid Fraud Control Unit.

In addition, we interviewed officials of a private insurance company, including a health care fraud investigator, as well as two beneficiaries and two doctors whose identities were used on fraudulent claims without their authorization or knowledge. Further, we reviewed case-related and public-record documents and reports, as well as reports and statistical information relating to this type of health care fraud.

We conducted our review from August 1998 through September 1999, in accordance with quality standards for investigations set forth by the President's Council on Integrity and Efficiency.

(600487)