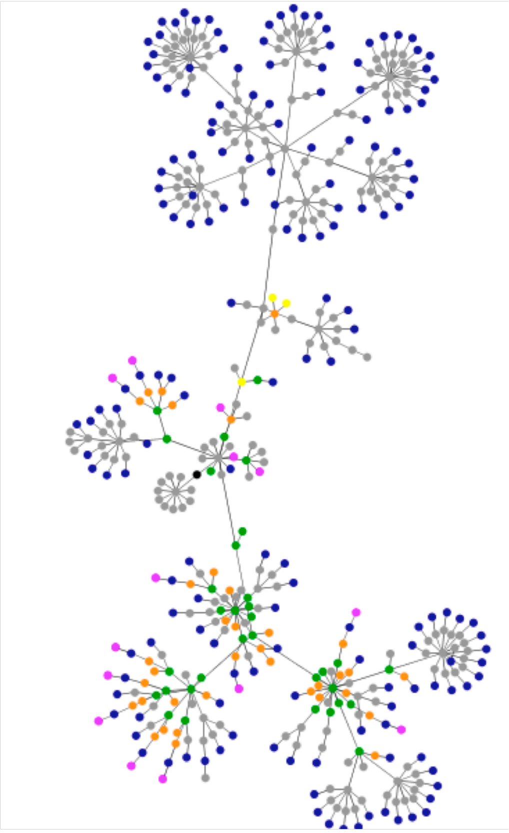
the Rise of Organized Crime in Health Care

Social Network Analytics Uncover Hidden and Complex Fraud Schemes

Summary: Social network analytics help to hone in on organized crime, which has made a significant entry into health care fraud, adding substantially to the tens of billions of dollars lost every year to scams. Expanded and sophisticated, this crime seriously affects individual consumers and threatens benefits. Government has redoubled its efforts to pursue the perpetrators, but conventional investigative methods and predictive claims models alone are not adequate to the problem. Social network analysis identifies relationship clusters using a variety of types of web-based and other data to zero on individuals and activities that represent fraud.

Modernized Approach to an Escalating Problem: By its weblike nature, organized crime has always lent itself to detection and prosecution through its social network. In the U.S., this held during periods such as the Prohibition, as well as the era when traditional mafia-type crime predominated, and since then with syndicates involved in such areas as gambling and narcotics. At no time has this strategy held truer than in an era when public data, including web-based information, can point out behaviors and associations between individuals — offering a combined matrix of indicators that high-powered computing and relational algorithms can analyze and illustrate clearly.

Organized crime typically conceals itself behind the façade of small businesses, the cover of corporations, or the anonymity of cyberwalls. Other industries, such as the financial markets have long dealt with complex crime structure, including operations that have offshore or international elements. The health care sector lags in efforts to deal with this problem, including in employing fraud and misuse solutions.[1]



Laying out fraud with graphing analysis. Social network analytics provide a different kind of data mining, summarized with graphing analysis — a visualization tool that makes significant connections among individuals and behaviors clearer and that correlates relationships between entities that would otherwise go unnoticed.

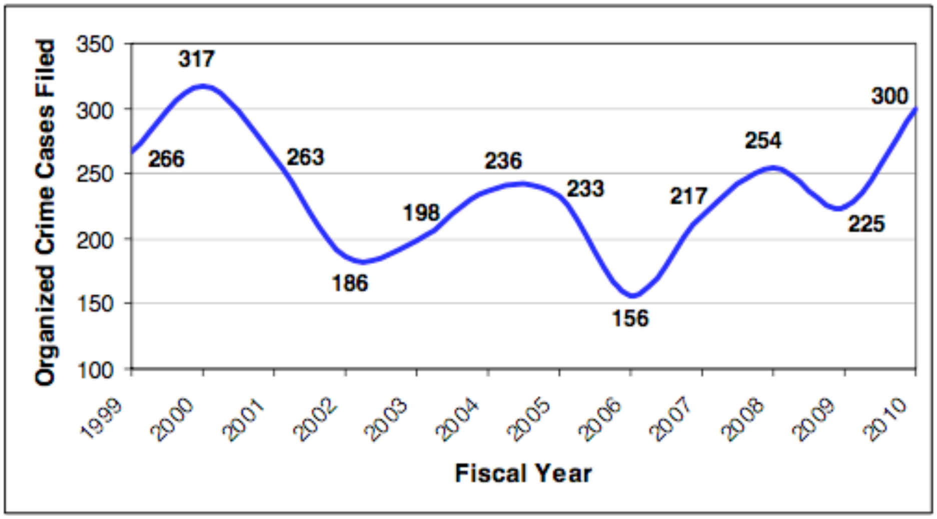
Migration of Organized Crime into Health Care

In Congressional testimony on April 2011, Gerald T. Roy, Deputy Inspector General for Investigations, Office of Inspector General (OIG), U.S. Department of Health & Human Services (HHS), said, "The most challenging and disturbing trend I have witnessed in my tenure . . . is the rise of criminal enterprises in health care fraud."[2] Criminal rings have realized the sheer scale of funds that move through health care. As a result, such health care fraud now goes well beyond the cases of abuse by individual health care providers or workers, or patients or government employees, of the kind known for decades. Instead, the new threat has international, national, regional, and metro-area aspects and is carefully conceived. Criminals set up hierarchical medical-scamming structures, and they view such rackets as safer, less violent, easier to hide, and less severely penalized than their traditional areas of crime activity.

In particular, sophisticated criminal networks are increasingly involved in fraudulent Medicare billing — in part due to the low barriers of entry to a federal program that allows any willing provider to deliver services for beneficiaries. The fraud extends to in all regions of the country, with hot spots in California, New York, and Florida, but also Texas, Michigan and many other states.[3]

How they do it: Scamming groups steal the identities of doctors, who bill for services, and of patients, whose beneficiary numbers entitle them to medical care and equipment. Historically, Medicare beneficiaries were not involved in fraud schemes. But today, crime team recruiters may earn a few hundred dollars for each a beneficiary they may pay a similar fee to for all Medicare or Medicaid information. The boss, who has set up a phony company or fake clinic using a legitimate provider's license and a provider number, then starts billing. Alternatively, a boss may set up fraudulent medical-service companies and pay gang members a few thousand dollars each to serve as nominee owners, to set up bank accounts, and fill out Medicare paperwork.

What's more, the scamming spreads by its own character. The names and numbers of hundreds of thousands of beneficiaries have been shared electronically among countless fraud perpetrators.[4]



Source: Data provided to CRS by the USAO.

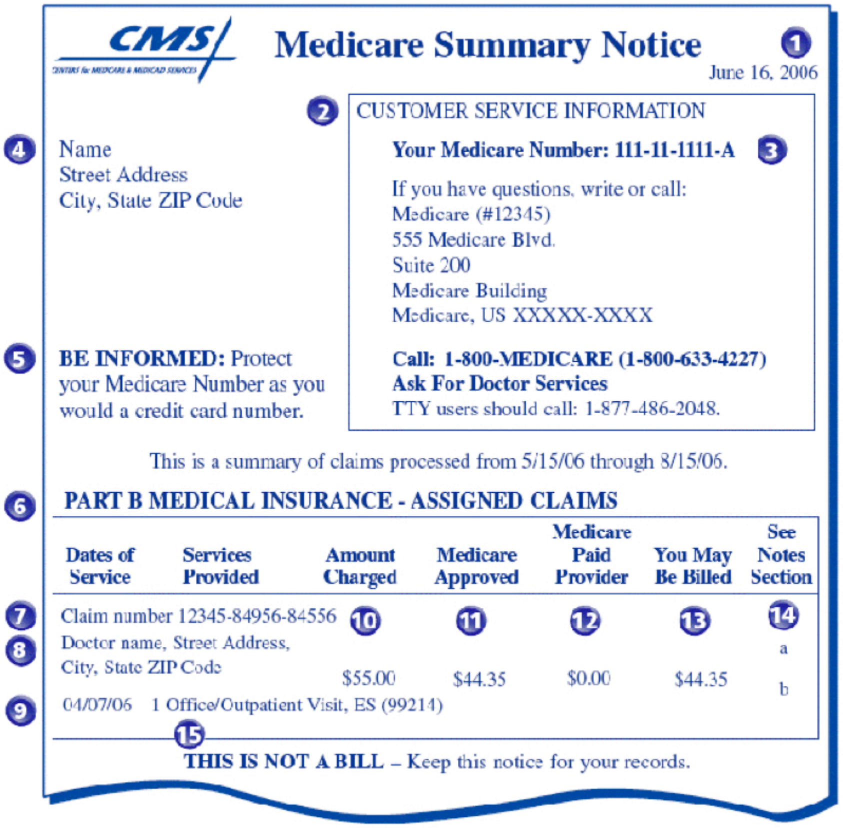
Organized crime cases filed with the U.S. Attorneys' Offices, FY1999-FY2010.[7]
With the nature and form of organized crime changing in the past half century, the number of cases filled against organized criminals dropped in the decade after 2000, only recently rebounding.

Healthcare fraudsters bill mostly for primary or specialty clinical visits and for home health care, though community mental health as well as physical & occupational therapy have also become recent targets. Wheelchairs, walkers, and hospital beds are the common foci of medical-equipment scams.[5]

Service fraud also includes "ping-ponging" (referring patients to other physicians in the same office), "gang visits" (billing for multiple services or collecting Medicaid recipients and bringing them in groups to clinics for medically unnecessary visits, sometimes paying or gifting them for such visits), and "steering" (directing patients to particular pharmacies). In some cases the rings have even staged automobile accidents to initiate false medical cases and then billed rehabilitation care, generating millions in total costs to insurance companies.[6]

In fall 2010, the FBI and HHS indicted 73 members of an Armenian-American organized crime enterprise involved in more than $163 million in fraudulent billing and operating out of more than a 100 different phony clinics in 25 states for the purposes of submitting Medicare reimbursements. Forty-four of the defendants were charged in Manhattan alone for racketeering, identity theft, and money laundering.[8] In the same month, DOJ and HHS indicted owners and senior managers of two Miami health care companies for an alleged fraud scheme involving approximately $200 million in Medicare billing for purported mental-health services. Four defendants of Latin-American background allegedly paid kickbacks to owners and operators of assisted living facilities and halfway houses in exchange for the facilities delivering patients for therapy. The patients allegedly received a portion of the kickbacks, and the company billed Medicare for services not medically necessary or not provided at all. [9]

image courtesy AARP



CMS CENTERS for MEDICARE & MEDICAID SERVICES

Medicare Summary Notice

June 16, 2006

Name
Street Address
City, State ZIP Code

CUSTOMER SERVICE INFORMATION

Your Medicare Number: 111-11-1111-A

If you have questions, write or call:
Medicare (#12345)
555 Medicare Blvd.
Suite 200
Medicare Building
Medicare, US XXXXX-XXXX

Call: 1-800-MEDICARE (1-800-633-4227)
Ask For Doctor Services
TTY users should call: 1-877-486-2048.

BE INFORMED: Protect your Medicare Number as you would a credit card number.

This is a summary of claims processed from 5/15/06 through 8/15/06.

PART B MEDICAL INSURANCE - ASSIGNED CLAIMS

Dates of Service	Services Provided	Amount Charged	Medicare Approved	Medicare Paid Provider	You May Be Billed	See Notes Section
Claim number 12345-84956-84556 Doctor name, Street Address, City, State ZIP Code		$55.00	$44.35	$0.00	$44.35	a b
04/07/06	1 Office/Outpatient Visit, ES (99214)					

THIS IS NOT A BILL – Keep this notice for your records.

Protecting consumers. The AARP and HHS have programs to educate the public to spot fraud and scams, to report suspicious activity, and to protect themselves. Consumers need to guard their cards, beware of free services that require a Medicare number, and scrutinize their statements.

As true in general of organized crime in the U.S. and worldwide, the health care fraud rings have also involve criminals of Cuban, Russian, Ukrainian, Asian, Eurasian, Italian, and Middle Eastern background — unfortunately opening concerns as well about a possible nexus between organized crime and terrorism. Government and private insurers have large intelligence gaps on these networks, even while they base their strategy for dismantling the rings on generating the most robust intelligence possible.[10]

A serious dollar loss: "They're hitting us and hitting us hard," said Timothy Menke, head of investigations for OIG at HHS [11] whose office estimates that losses for inappropriate government billing for health care services each year at roughly $60 billion, of which the government recovers less than ten percent annually.[12] Other estimates place this number closer to $200 billion.[13] For public and private payers together, the National Health Care Anti-Fraud Association (NHCAA) calculates that fraud costs the system between $75 billion and $250 billion a year.[14]

Medicare and private insurers pay millions of claims every working day valued at billions of dollars *per day*. Prompt-pay regulations require them to remit submitted claims within a set period of time. Due to resource limitations, Medicare conducts medical review on less than three percent of all submitted claims before paying them.[15]

Real impact on people: Criminals may perceive health care fraud as less risky to themselves but it's not less risky to patients and society. It directly escalates the cost and endangers the quality of health care for every American. Health care fraud and abuse not only contributes to higher insurance premiums, but every dollar paid in fraudulent or abusive claims reduces the amount of money available to improve the quality of care for those incurring legitimate expenses.

This expanding situation can especially affect seniors and persons with disabilities or chronic diseases who need supplies and care. Criminal enterprises posing as pharmacies, for example, bilk health care out of millions of dollars by charging Medicare, Medicaid and private pharmacy benefits for fake prescriptions. These "phantom pharmacy" or “pill mill” schemes operate from a real address using a stolen doctor ID along with patient insurance ID numbers to write fraudulent prescriptions for expensive drugs never actually prescribed or dispensed. Each fake claim can bring in thousands of dollars. With the income, criminals may operate in groups opening a number of false pharmacies, and then money laundering the proceeds to oversees accounts.[16]

The experience is also not pleasant for those directly exposed to this criminal activity. Criminals have threatened investigators and attacked witnesses.[5] They unnecessarily transport patients and subject them to unneeded care that may carry its own risks. Furthermore, medical identity theft can prove expensive to its victims — less in direct financial liability than in terms of compromised medical and insurance records that cause problems later. Some Medicare recipients apply for long-term care or other insurance and find they do not qualify because their medical records include fraudulent treatments and tests. In addition, when scams get particularly popular, Medicare cracks down on eligibility, making it more difficult for those who truly need the help.[17]

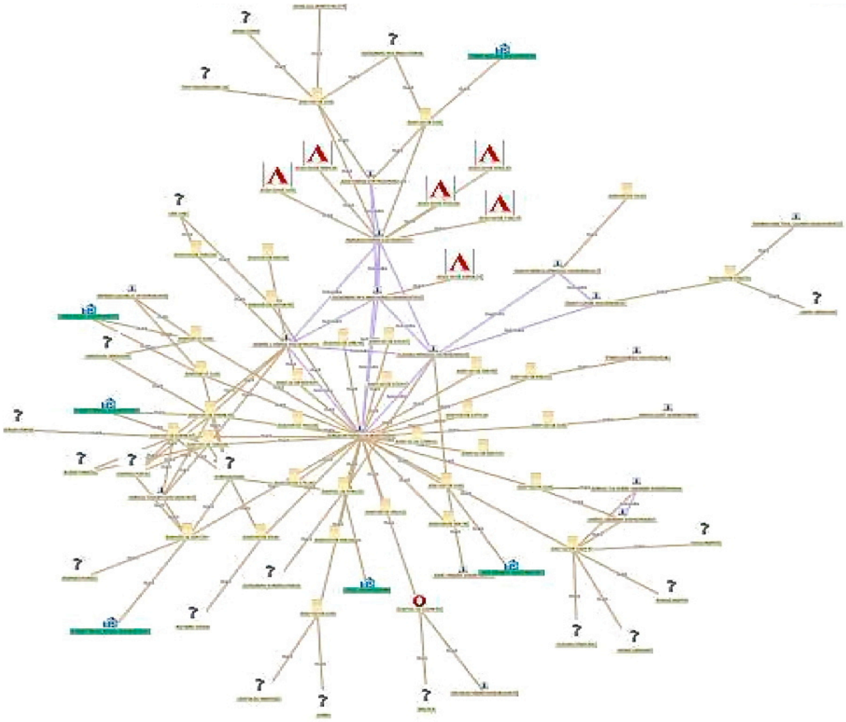
Organized criminal healthcare fraud directly escalates the cost and endangers the quality of health care for every American.

What the Government Has Done so Far

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) set up a national Health Care Fraud and Abuse Control (HCFAC) program under the direction of the OIG and HHS to coordinate federal, state, and local law-enforcement activities. Well over a half-billion dollars in appropriations to specifically fund these anti-fraud efforts in FY 2010 included $268 million to CMS, $208 million to OIG, $130 million to the FBI, and $43 million to the USOA.[18]

The perception among criminals that penalties for health care fraud are far less severe than those imposed for their conventional types of crime may have been true in the recent past, but changes to sentencing guidelines have closed that gap. Penalties for charges recently have included, in addition to repayment, a $500,000 fine and life in prison.

James Sheehan arguably the nation's best-known prosecutor of health care fraud has been called a visionary in his work as the former New York Medicaid Inspector General. His team recovered more than $1.2 billion in improper Medicaid payments in four years starting in 2006 and helped his state’s Medicaid program avoid paying $2 billion more. His agency has excluded nearly 4,900 providers and cut off an additional 1,763 — more than any other state. He had similar successes in Philadelphia. Sheehan’s approach evolved to an emphasis on solving these problems internally first, within providers, payers, and government agencies, rather than have the enforcement community fix them, moving from a prosecutorial stance to a preemptive partnership.[19]



Layering in other clues. Social network analytics provides another whole aspect and adjunct to the pursuit of fraud, putting intelligence gathering in a relationship context that highlights associated risk. Graphing analysis displays degree of association and confidence for each relationship linkage shown. Variables computed can include personal information as well as data on businesses, assets, and properties. Graphing analysis gives context to those connections and quickly helps investigators understand concealed relationships — in order to begin meaningful investigations.

And yet this requires knowing where the problems are. Furthermore, pursuit of flagrant criminal activity must proceed in parallel and apace. For that latter purpose, HHS and DOJ launched the Health Care Fraud Prevention and Enforcement Action Teams (HEATs). HEAT Strike Forces take advantage of increased tools and resources, and sustained focus by senior level leadership. In geographic areas at high risk for Medicare fraud, the Strike Forces pursue a technologically sophisticated and collaborative approach. Instead of relying primarily on insiders with knowledge of schemes, though, Strike Force cases are data driven, using technology to pinpoint fraud hot spots, starting with identifying inexplicable billing patterns as they occur.

"Much of our attention has been focused on obtaining real-time data," says Menke about the HEAT initiative, adding that additional "real-time data access would enable us to more efficiently conduct field surveillance, electronic monitoring, and issue search and arrest warrants." In Congressional testimony, he adds that the more current the data, the more effective agents can be in:

- 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 [to] quickly and accurately locate evidence of a crime before perpetrators destroy, alter, or manufacture information; and
- planning an arrest warrant [to] quickly determine the location of a subject before the subject is alerted to [the] investigation and has an opportunity to flee or prepare for [law enforcement] arrival if the subject does not intend to cooperate.[18]

Technology to Seek Out Organized Crime in Health Care

Traditional methods alone are not adequate: Leaders and decision makers need to question whether the tools they have allocated to combat organized crime are still effective for countering today's risks. Despite the best efforts of domestic and international working groups and task forces, fraud by organized crime remains a massive problem. Conventional efforts to stop such crime, while yielding more recoveries each year, simply are not enough and are recapturing only a small percentage of the losses. Experts estimate that a more preventive, proactive model could net Medicare alone as much as $70 billion a year in savings,[20] potentially providing a major opportunity to slow spiraling health care spending as a percent of GDP.

New provider enrollment rules under the Affordable Care Act seek to ensure that providers and suppliers are screened according to risk of fraud, waste, and abuse before being allowed to enroll in federal programs. For now though, payers accept and pay the vast majority of claims without sufficient analytics to determine their legitimacy — instead of catching the fraud before a payment goes out the door. Pursuit then has to take place after the fact. All agree on the need to move beyond this "pay and chase" approach.

Legislative efforts to fight health care fraud continue and could require CMS to apply a comprehensive pre-payment predictive process to all claims.[21, 22] Predictive modeling techniques can accomplish this by looking at:

- *identity integrity*. These analytics verify and authenticate the identity of the provider or supplier, and ensure that their eligibility conforms to requirements.
- *claims legitimacy*. These analytics set up screens to highlight outlier patterns that may represent fraudulent activity.

But even these steps are often not enough to close in on and define organized groups committing health care fraud. For that, an anti-fraud program needs to also add *social network analytics,* which take advantage of the collusive nature of this criminal activity.

How social network analytics work — finding links and hidden patterns: New technology, called social network analytics, can help identify relationships and interactions within clusters of individuals, including:

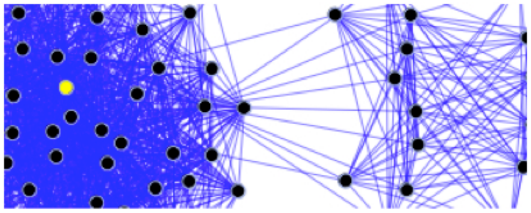
- patient relationships with known perpetrators of healthcare fraud;
- links between recipients, businesses, and assets, as well as relatives and associates;
- links between licensed and non-licensed providers;
- and inappropriate relationships of employees, suppliers, and partners with patients and providers.

Advanced technology, using powerful computing and association software, can cluster diverse variables to reveal organized activity. Additionally, access to vast public records databases that go beyond phone and address information (and that track web-based behaviors and information) make connections between entities, assets, and people even more transparent. Social network analytics can thus focus in to reveal the roots and tentacles of fraud within a provider network.[23]

LexisNexis® analytics consider thousands of attributes to identify data patterns that can be used as indications about the level of risk associated with a particular provider. The information searched includes more than 34 billion proprietary and non-proprietary public records, refreshed daily, that can be analyzed against entries in client data.[24] The industry's most powerful internal data-linking analysis and technology relies on a massive parallel-processing open-source computing platform (the High Performance Computer Cluster). The approach derives public data relationships from

Social power. Large-scale graph analytics, generally thought to be the domain of companies like Google, now see expanded use for exposing unseen patterns:

- Twitter, FaceBook, LinkedIN and other social-network platforms uses graph analysis-type paradigms to determine who's connected to whom in the cybersphere.
- Google uses graph analysis to power its page-rank and ad-targeting features.
- **LexisNexis®** uses graph analysis to resolve identities and combat fraud.



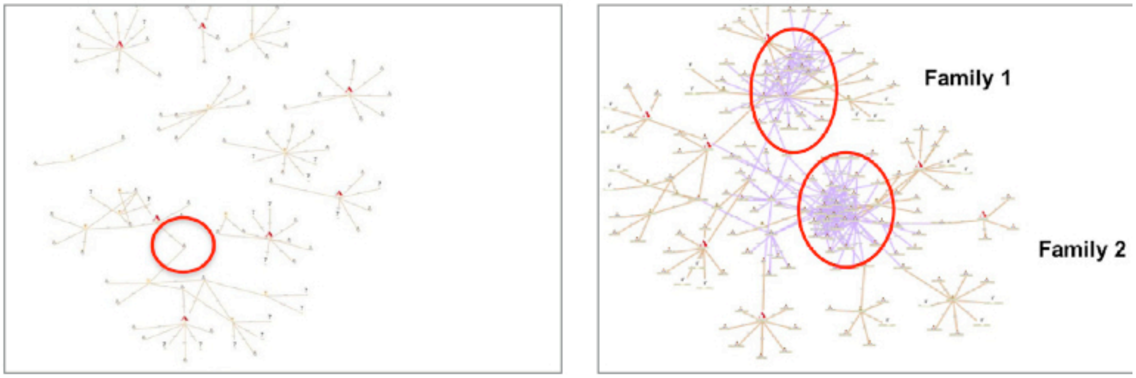
the LexisNexis database of approximately 50 terabytes for the entire U.S. population.[25]

Social network analytics use algorithms that aggregate linkages into high-value clusters of interest, illustrated by graph analysis *(see figures)*. Maps of transportation systems or disease epidemics, or of connections that the web itself makes among subject matter, are examples of graph analyses. Graph analysis built on social relationships ingests and integrates massive volumes of disparate data to determine who and what go together.

In pursing medical-fraud criminals, the LexisNexis social network analytics solution can look at clusters of the most significant statistics and, for example, additionally query how many beneficiaries, providers, or other individuals are, say, living in expensive residences, own expensive property, drive expensive cars, or are contacts of medical businesses, further combining these variables with benefit details, dollar amounts, and treatment history.

What social network analytics produce: The Omnibus Crime Control and Safe Streets Act of 1968 granted law enforcement the ability to wiretap suspects and their associates, revolutionizing the pursuit of organized crime. Social network analytics offers a 21st Century version of this leap, but one hugely more robust. What's more, such analysis doesn't require a warrant and it updates immediately when new proprietary or public information becomes available.

More data, combined with algorithm-and-computing solutions that can process it, have now made social network analytics an option for public and private insurers and law-enforcement offices. Indeed, by permitting the analysis to use both internal and external data, the approach allows payers and prosecutors for the first time to stay one step ahead of perpetrators by asking: What behaviors are predictive of fraud? This powerful tool exposes ringleaders and brokers who may not directly participate, and it can potentially be helpful in soliciting qui tam (or whistleblower) complaints, which are important to many prosecutions.



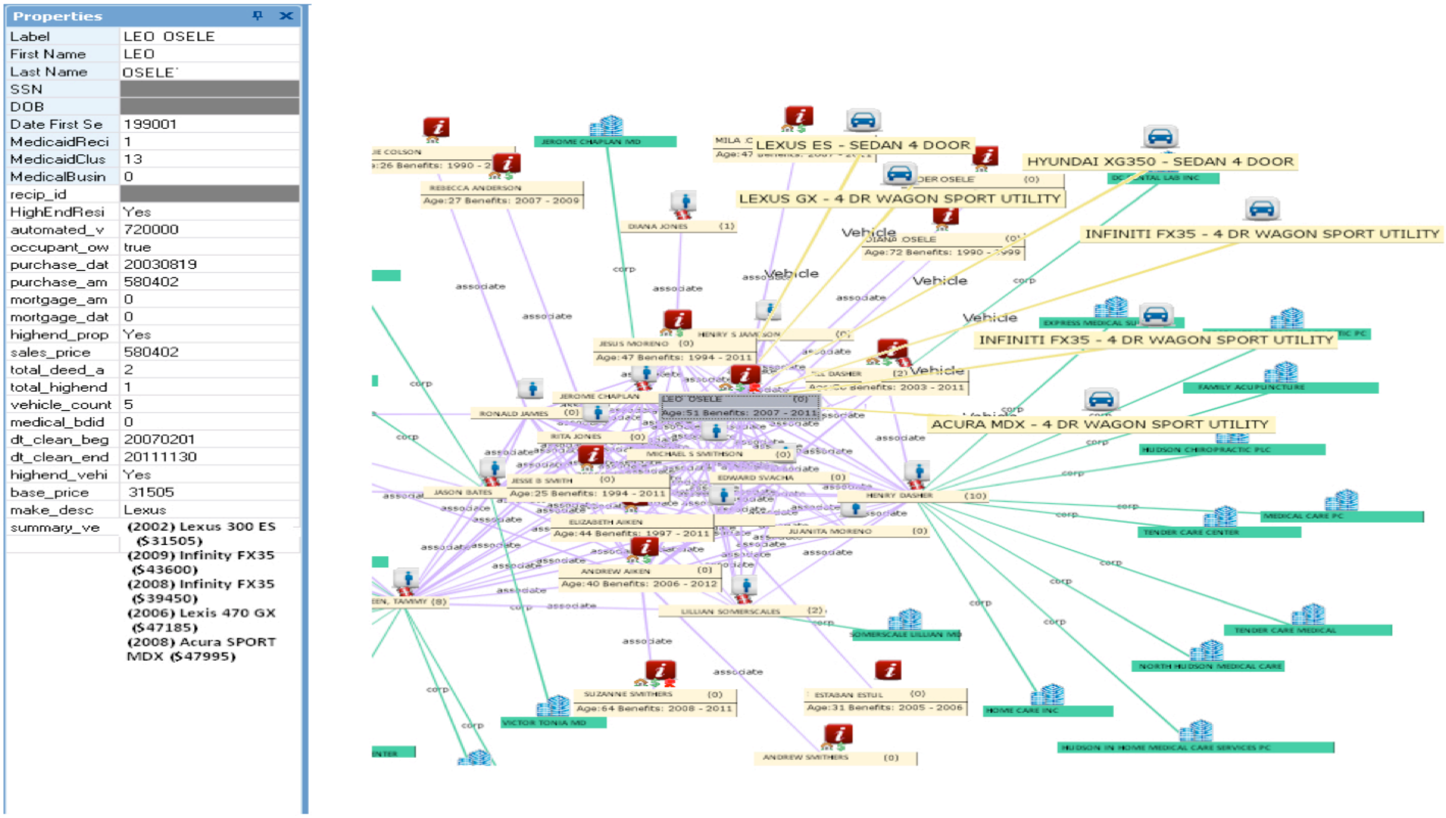
Adding other dimensions to enhance resolution. Using its own internal data and traditional linking methods, a private insurer found just one link between seven insurance fraud schemes, representing hundreds of suspect claims. But employing advanced capabilities, LexisNexis linked the insurer's internal data to the a public-records database and identified 11 additional potential fraudulent schemes directly related to the original seven, as well as two families that appeared to be at the center of the activity.

Technology Hones on Healthcare Criminals

Like any grand, newer communication medium, social networks based on web-, computer- and portable-device user platforms serve purposes both good and ill. They provide hundreds of millions worldwide with connectedness. Their capacity to spread positive and constructive information exists simultaneously with their capacity to serve harmful and nefarious purposes. In 2011, they helped to promote democracy movements in the "Arab Spring," while they also helped organize riots in London. Like it or not, scanning, filtering, and sifting through this kind of information has become essential to staying on top of any organized activity or behavior that undermine society.

Federal entities can use social network analytics in conjunction with the single searchable database of all paid Medicare claims that DOJ and HHS have created, just as private insurers can with their own proprietary databases. And the effort is well worth it. The HCFAC program has proven the value of a collaborative, data-intensive approach, with HHS reporting a return of approximately $7 for every $1 invested in pursuing Medicare fraud through the program for the most recent year average.[3] Likewise, U.S. states invested roughly $200 million in Medicaid integrity programs last year, with recoveries approaching $1.5 billion.[15]

Enhanced intelligence technologies and solutions are on every authority's wish list for combating health care fraud. HHS's Center for Program Integrity (CPI)



Properties

Label	LEO OSELE
First Name	LEO
Last Name	OSELE
SSN	[redacted]
DOB	[redacted]
Date First Se	199001
MedicaidReci	1
MedicaidClus	13
MedicalBusin	0
recip_id	[redacted]
HighEndResi	Yes
automated_v	720000
occupant_ow	true
purchase_dat	20030819
purchase_am	580402
mortgage_am	0
mortgage_dat	0
highend_prop	Yes
sales_price	580402
total_deed_a	2
total_highend	1
vehicle_count	5
medical_bdid	0
dt_clean_beg	20070201
dt_clean_end	20111130
highend_vehi	Yes
base_price	31505
make_desc	Lexus
summary_ve	(2002) Lexus 300 ES ($31505) (2009) Infinity FX35 ($43600) (2008) Infinity FX35 ($39450) (2006) Lexis 470 GX ($47185) (2008) Acura SPORT MDX ($47995)

Provider-behavior analysis targets interventions. LexisNexis applied social network analytics to both information provided by the State of New York and public information in its expansive database in order to identify (a) relationships between a group of New York Medicaid recipients living in high-end condominiums located within the same complex and (b) any links those individuals might have to medical facilities or others providing care to New York Medicaid recipients.

has already piloted use of a fraud-detection tool that links publicly available data sources in order to conduct network analysis for specific Medicare providers.[3] Meanwhile, CMS is soliciting new technology for such efforts.

Health care fraud conducted by organized crime is a threat to consumers because of its ability to exploit programs, budgets, and resources. Benefits are under siege by scammers, just as some 70 million Baby Boomers approach retirement age.

"What's disturbing now is we're seeing a viral nature of health care fraud going across the United States," says Menke.[26] However, it's that very virulent nature of this activity that make these criminal groups vulnerable. Scammers expose themselves if authorities look closely enough, especially as perpetrators interface with each other, their co-conspirators, and their victims. Social network analytics make this activity much easier to see.

[1] Enterprise Fraud and Misuse Management Solutions: 2010 Critical Capabilities, 29 October 2010, Gartner, Inc.

[2] Congressional Documents and Publications, April 5, 2011, Federal Information and News Dispatch, Inc

[3] The Department of Health and Human Services and The Department of Justice, Health Care Fraud and Abuse Control Program, Annual Report for Fiscal Year 2010, January 2011

[4] A Perspective on Fraud, Waste, and Abuse Within The Medicare and Medicaid Programs, Testimony of Gerald T. Roy, Deputy Inspector General for Investigations, Office of Inspector General, U.S. Department of Health & Human Services

[5] Congressional Quarterly HealthBeat, March 2, 2011 Medicare Fraud Going 'Up, and Up, and Up,' Republicans Charge

[6] The Globe and Mail (Canada), December 27, 2010 Bumper To Bumper Fraud; Grant Robertson And Tara Perkins Examine Staged Accident Rings, The Collusion Of Some Health-Care Clinics And The Huge Payments Drivers Are Bearing To Absorb The Growing Costs Of Criminality That Insurers And Regulators Seem Unable To Stop

[7] Organized Crime in the United States: Trends and Issues for Congress, Kristin M. Finklea, Analyst in Domestic Security, Congressional Research Service, December 22, 2010

[8] US Fed News, October 14, 2010, 73 Members, Associates Of Organized Crime Enterprise, Others Indicted

For Health Care Fraud Crimes Involving More Than $163 Million

[9] US Fed News, October 23, 2010, 2 Miami Corporations And Four Individuals Indicted For Health Care Fraud Scheme Involving Approximately $200 Million In Medicare Billing

[10] Strategy to Combat International Organized Crime, U.S. Department of Justice, April 2008

[11] October 22, 2009|By Allan Chernoff and Sheila Steffen, CNN.com, http://articles.cnn.com/2009-10-22/justice/medicare.organized.crime_1_organized-crime-medicare-patients-medicare-and-medicaid?_s=PM:CRIME

[12] Investigation of Health Care Fraud, U.S. Department of Health and Human Services, Office of Inspector General

[13] October 2009 Thomson Reuters Report http://www.reuters.com/article/2009/10/26/us-usa-healthcare-waste-idUS TRE59P0L320091026

[14] Managed Healthcare Executive, April 2011, Insurers Want MLR Policies To Include Anti-Fraud Efforts

[15] PROGRAM INTEGRITY, August 24, 2010
Bob Foster, CMS Atlanta

[16] CNNMoney.com, June 20, 2011

[17] The New York Times, October 30, 2010, Be Alert to Protect Yourself Against Medicare Fraud

[18] Testimony before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, March 4, 2010, Testimony of: Timothy J. Menke, Deputy Inspector General for Investigations Office of Inspector General, U.S. Department of Health & Human Services

[19] Philadelphia Inquirer, 8/31/11

[20]

http://www.thefiscaltimes.com/Articles/2011/03/10/Medicare-Fraud-A-70-Billion-Taxpayer-RIpoff.aspx

[21] Grassley Fights Fraud in Medicare and Medicaid, March 2, 2011, Sen. Chuck Grassley (R-IA) News Release Federal Information and News Dispatch, Inc. Congressional Documents and Publications

[22] Congressional Documents and Publications
June 15, 2010, House Ways and Means Subcommittee on Health Hearing; Hearing on Reducing Fraud, Waste and Abuse in Medicare; Testimony by Rep. Roskam, Peter J. - (R-IL), Federal Information and News Dispatch, Inc.

[23] Bending the Cost Curve: Analytic Driven Enterprise Fraud Control, LexisNexis white paper, 2011

[24] LexisNexis® Social Network Analytics for Health Care 2011

[25] presentation, World Health Care Congress, Bill Fox, JD, MA, Senior Director Health Care, LexisNexis Risk Solutions

[26] National Public Radio interview, January 16, 2010 http://www.npr.org/templates/story/story.php?storyId=122645717