Paper 176-2011

Fighting Fraud in a Pre-Payment Environment

Julie Malida & Greg Henderson

SAS Institute Inc, Raleigh, North Carolina

ABSTRACT

In the U.S. Health Care industry, dollars lost to fraud each year are 3-10% of total U.S. Health Care spending. Adding in waste and abuse (where the intent to falsify information for financial gain is never proven), these estimates approach 1/3 of total health care spending. In Europe, the fraud estimate is 6% of health care spending, in Canada, 2% of health care spending. It is a worldwide issue. As such, health care fraud is a lucrative business and organized crime, cross-border schemes, and multi-party collusion have moved full force into health care.

The health care industry loses 100 times more than the credit card industry does due to fraud, and yet the investment on fraud fighting solutions in health care is one tenth as much as the credit card industry. Most payers of health care claims (private payers as well as governments) are still detecting and investigating fraud after the claim is paid, known as “pay and chase”. However, there is a growing recognition that detecting and stopping fraud before the claim is paid, known as “pre-payment” is the way of the future.

Fighting fraud pre-payment by having the right detection tools in place to identify leads and prioritize them quickly is a key. Private payers were the first to embrace the concept of moving the screening process further up in the transaction life cycle, but government entities are now recognizing the benefits of this approach as well.

INTRODUCTION

Upcoding of evaluation and management services rendered during an office visit … unbundling of lab services that should be billed using a single lab-panel code … loaning a health insurance card to a family member not covered by the plan … submitting medical charges for nonexistent conditions or unnecessary procedures. It’s all small potatoes, a victimless crime, fair compensation for spiraling premiums, deductibles and negotiated, lower reimbursements to health care providers for managed care, right?

That attitude seems to prevail among patients, providers and suppliers these days. Nearly one in four Americans said that it is OK to defraud insurers, according to a 2003 Accenture survey[1]. About one in 10 respondents agreed that it is OK to submit claims for items that are not lost or damaged, or for personal injuries that didn’t occur[2]. More than one in three Americans said it’s OK to exaggerate insurance claims to make up for the deductible, according to the Insurance Research Council[3].

[1] Coalition Against Insurance Fraud. “By the numbers: fraud stats.” http://www.insurancefraud.org/stats.htm

[2] Progressive Insurance, 2001.

[3] Insurance Research Council, 2000.

These attitudes cost the industry billions of dollars each year. And what costs health care payers also costs the rest of us. According to the National Health Care Antifraud Association (NHCAA), health care fraud, waste and abuse strips nearly $70 billion from the industry each year[4] – losses that must be made up in premiums. The NHCAA estimate represents 3 percent of the $2.26 trillion dollars spent on health care annually in the United States. Since insurance fraud is hard to detect, these figures can only hint at the magnitude of the problem, with some loss estimates ranging as high as 10 percent of health care expenditures, or $230 billion annually. The European Healthcare Fraud & Corruption Network (EHFCN) estimates almost the same figures ($132 billion annually).

WHATEVER THE DOLLAR FIGURE, FRAUD IS A BIG PROBLEM

The impact of fraud, waste and abuse on payers, whether insurance companies, government agencies or self-insured employers, is enormous. Fraud losses weaken a payer's financial position, with fraud loss estimates rivaling net income. Fraud losses feed the escalating care cost curve, undermining a payer's ability to offer its most competitive rates to customers, eroding profitability and increasing pressure to ratchet down provider payment rates. In the end, fraud losses lead to higher premiums for contract holders and lower payment rates for providers. In this "victimless" crime, everybody pays the price.

Technically, for an action to be labeled "fraud," intent must be proven in a court of law. For purposes of this paper, we will use the term "fraud" to mean fraud, waste or abuse, regardless of whether intent is proven. Government agencies in the United States and Europe have responded with new regulations and centralized fraud bureaus. Health payers have responded by establishing special investigative units (SIUs) to detect and prevent fraud. Yet the problem continues to grow significantly in recent years.

- *According to the National Health Care Antifraud Association, health care fraud, waste and abuse strips nearly $70 billion from the health care industry each year.*[5]

Why is that? For one, many health payers believe that it is too expensive to detect fraud, and they simply accept a certain amount of fraud loss as a standard cost of doing business. With the increased focus on customer satisfaction and regulatory requirements for timely payment, health payers are understandably reluctant to stall claims processing to investigate a hunch. Likewise, they do not want to mistakenly target for investigation a legitimate claim and an honest contract holder, provider or supplier. Compounding the issue is a reluctance to disturb the often-contentious payer/provider relationship that results from the provider network negotiation process.

Second, health payers often operate with data systems and technical analysts that reside in silos, making it difficult or impossible for staff with expertise in legal investigation or clinical coding to assemble a complete view of claims history and member or provider data without assistance from other business units. The result has been a reliance on retrospective, manual review of claims that have already been paid – the implication being that money has already left the health payer and is in the hands of those that would abuse or defraud the system.

To make matters worse, the state-of-the-art means of lead identification has been fraud hotlines and rules engines. The former relies on a member of the public becoming aware of a fraud or abuse scheme and demonstrating a willingness to report it to an insurance company, employer or government agency. The latter looks for claims that conform to previously identified fraud or abuse schemes, but suffers from an inability to adapt to even slight modifications of those schemes, much less new schemes.

---

[4] National Health Care Antifraud Association. "The Problem of Health Care Fraud." http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=TheProblemOfHCFraud, 2009.

[5] National Health Care Antifraud Association. "The Problem of Health Care Fraud." http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=TheProblemOfHCFraud, 2009

When abuse or fraud is finally confirmed, the payer must engage in costly efforts to recover the associated losses. The resulting “pay-and-chase” cycle only serves to add administrative costs to fraud and abuse losses, and emboldens those that seek reimbursement for falsified claims.

n *How can such a company identify multiple entities that are operating in collusion, or identify patterns that would only be suspicious when viewed from a broader perspective?*

Amid these dynamics, fraudsters have become more resourceful than ever. Recruitment and transport of patients for bogus procedures, trading narcotics in exchange for member IDs, identity theft, doctor and pharmacy shopping - all result in claims that appear legitimate when viewed in isolation. Timely payment requirements, automated claims processing and lack of widespread, prepayment fraud detection capabilities have helped make health care fraud a low-risk, high-return criminal activity - second only to tax evasion in economic crime. Today’s fraudsters also have a good understanding of fraud detection systems, frequently recruit insiders into their schemes, and actively test and exploit thresholds and detection rules to avoid exposure.

THE MANY FACES OF HEALTH CARE FRAUD

Part of the problem in detecting and reducing health care fraud is that the perpetrators often do not fit what would normally be considered as a “criminal profile.” Sheer numbers wouldn’t tell the whole picture either, because there are two distinctly different types of fraud:

- Opportunistic fraud is usually perpetrated by an individual who simply has a chance to inflate the services represented on a claim or to obtain the same services from multiple providers. This person might know an insider but generally isn’t operating with an insider’s knowledge of the insurer’s fraud detection systems or thresholds. Opportunistic fraud is commonplace, but the dollar amount per incident is relatively low. Individuals with no prior criminal history may begin to duplicate scripts in order to fill multiple prescriptions for the same drug, either to abuse the medication or to sell it on the street. Highly educated professionals, including doctors, nurses and pharmacists, may give in to the temptation to increase revenue by billing for exaggerated services or procedures that were not performed.

- Professional fraud is often perpetrated by organized groups with multiple, false identities, targeting multiple organizations. These criminals know how fraud detection systems work, and they routinely test thresholds to stay just under the radar. These crime rings often place or groom insiders to help them defraud health payers through several channels at once. The incidence of organized fraud is lower than ordinary health care fraud, but the dollar amount per scheme is far greater. However, it is only when viewed from a network perspective, which reveals the hidden linkages between the individuals involved, that the true financial magnitude of the scheme can be assessed.

n *Today’s fraudsters also have a good understanding of fraud detection systems, frequently recruit insiders into their schemes, and actively test and exploit thresholds and detection rules to avoid exposure.*

COMBATING HEALTH CARE FRAUD

Traditional fraud and abuse detection systems using business rules, telephone tip lines and profiling focus on opportunistic fraud. Most systems in place only detect fraud at the individual customer or claim level, and overlook more organized criminal activity. But organized crime rings are growing, and so is the sophistication and velocity of their attacks. Electronic claims submission makes it easy for professional criminals and revenue maximizers alike to hide and shift identities and relationships, to test and evolve their tactics – and to disappear after a few successful transactions. Payers need more than traditional methods and systems if they expect to manage this new breed of fraudsters and reverse this trend.

EVOLUTION OF THE WAR ON HEALTH CARE FRAUD

The 1980s: The early years

Insurance and fraud have likely gone hand in hand since the industry's beginnings in the 17th century. The advent of health insurance, with the complexity resulting from the possibility of multiple health care transactions per episode of illness, opened new opportunities. However, fraud received little attention until the 1980s. By this time, rising health care premiums, and the focus on health care cost containment, made fraud a more difficult issue for health payers to ignore. To tackle this growing problem, health payers initially began implementing *simple rules-based techniques and telephone fraud hotlines* to identify specific patterns and highlight activities that looked suspicious. The National Health Care Anti-Fraud Association was created by health payers to provide a vehicle for information sharing and education around health care fraud awareness. And later, Europe created the EHFCN.

The 1990s: IT revolution

In the 1990s, insurance and financial industry swindles were growing bigger, more complex and harder to detect. The automation of health care claims processing created new opportunities for fraudsters and abusers to rack up improper payments. Organized crime rings began to recognize the relatively low risk associated with health care fraud as compared to other criminal activities. The industry responded with stronger anti-fraud legislation on behalf of state fraud bureaus – and the creation and increased adoption of SIUs within health insurance companies. Still, health payers lagged behind many other industries with respect to adoption of technology and advanced decision support methods, and few technological advances were brought to bear on the problem of health care fraud and abuse.

n *Health care payers need more than traditional methods and systems if they expect to manage the new breed of fraudsters and reverse this trend.*

Today and beyond: Sophisticated and multifaceted approaches

Rapid advances in technology enable health payers to use more powerful techniques to not only detect fraudulent activity, but to prevent it. For example:

- *Predictive modeling* compares claims to baselines or thresholds to create fraud-propensity scores.
- *Social network analysis* shows links between entities to uncover abnormal claims patterns.

It is impossible to predict future trends in fraudulent activities other than to say that schemes will continuously evolve. Fraudsters continually become more inventive and resourceful – and evasive. Push hard in one area, and they will shift their focus somewhere else. Change thresholds and models, and they will soon discover the new limits and skirt around them.

Payers have the means to become more inventive, adaptive and resourceful too. By using a combination of approaches – and by exploiting the advantages of analytics-based techniques – they have more opportunity than ever to recognize fraud and stop it before it occurs.

KEY TECHNIQUES FOR DETECTING AND PREVENTING FRAUD

There is no one bulletproof fraud or abuse detection technique. Multiple techniques, working in concert, offer the best chance for detecting both opportunistic and professional/organized fraud. A hybrid approach, which integrates knowledge of existing fraud schemes, powerful predictive analysis techniques, and comprehensive triage and case management capabilities, is necessary in order to:

- Adapt to continuously evolving fraud and abuse schemes.
- Offer prepayment detection of suspicious claims with high certainty.
- Provide enough efficiency to enable triage of large volumes of claims.
- Automate the detection of multi-entity fraud and abuse schemes.

Let's take a look at prevailing techniques that insurers and third-party administrators should include in their arsenal of anti-fraud strategies.

n *Rapid advances in technology enable insurance companies to use more powerful techniques to not only detect fraudulent activity, but to prevent it.*

DYNAMIC RULES ENGINES

Rules-based systems test each transaction against a predefined set of algorithms or business rules to detect known types of fraud or abuse based on specific patterns of activity. These systems flag any claims that look suspicious due to their aggregate scores or relation to threshold values.

For example, a business rule might target a claim for closer inspection if it exceeds a certain dollar amount, involves multiple medical procedure codes when a single code should be used or shows services inconsistent with medical history. Similarly, claims could be red-flagged if the claimant has submitted an unusual number of claims in recent years, recently instituted or changed benefit plans, or provided similar services to multiple family members within a narrow time window. Red-flagged claims are then evaluated more thoroughly by experienced investigators.

The advantage of the rules-based approach is its simplicity. After initially configuring the business rules, it is easy to match activities to individuals with very little investment or training. Unfortunately, there are many disadvantages to a manual, rules-based system, which puts the burden of triage on overworked investigators. Rules engines may uncover large numbers of suspicious claims, many of which will turn out to be false positives. In addition, fraudsters can easily learn the rules and devise ways to work around them. Furthermore, rules are based on past fraud experiences, so they fail to detect new fraud techniques. In order to maximize utility, investigators must have the ability to add to, or modify, the rules repository as new rules are discovered rather than waiting for annual commercial release schedules.

DISCOVERY METHODS: GOING BEYOND KNOWN FRAUD AND ABUSE SCHEMES

Anomaly Detection

Report events that exceed a threshold for a particular claims benchmark.

With anomaly detection, key performance indicators (KPIs) associated with tasks or events are baselined and thresholds set. When a threshold for a particular measure is exceeded, then the event is reported. Outliers or anomalies could indicate a new or previously unknown pattern of fraud. On the plus side, this type of tool is straightforward, easy to implement and intuitive to understand. On the negative side, it can be difficult to determine what to measure, what time period to use and appropriate threshold levels. Set thresholds too high, and too many fraudulent claims could slip through the system; too low, and you risk wasting time, alienating members and providers, and paying late-payment penalties. Statistical analysis takes the guesswork out of threshold setting by empirically determining “normal” ranges for predetermined metrics.

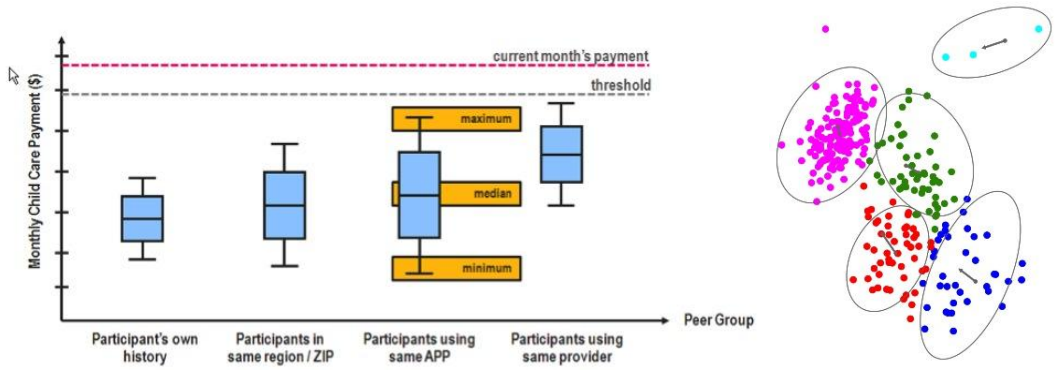

Figure 1: Examples of how anomalies and outliers are detected with KPIs.

Predictive Modeling

Use data mining tools to build models to produce fraud-propensity scores.

In recent years, many industries have turned to predictive modeling processes, using the power of statistical analysis to discover previously unknown fraud schemes linked to unidentified metrics. This method of fraud scheme discovery uses data mining tools and builds programs that produce fraud-propensity scores. Claims are automatically scored for their likelihood to be fraudulent and made available for review.

Predictive modeling tends to be more accurate than other fraud detection methods. Information can be collected and cross-referenced from a variety of sources. This diversity of resources provides a better balance of data than the more labor-intensive, rules-based system. More importantly, the schemes that are discovered do not depend on the upfront assumptions made regarding the metrics that may be associated with fraud. Instead, the data mining and predictive modeling process statistically determines key metrics that are associated with claims that have a high fraud-propensity score.

Predictive models do exhibit degradation with age. As those that abuse or defraud the health care system adopt new approaches, models must be updated, or “retrained,” to reflect new patterns. Once again, statistical analysis can be used to identify the point at which retraining is necessary. In spite of these limitations, predictive modeling shows great promise.

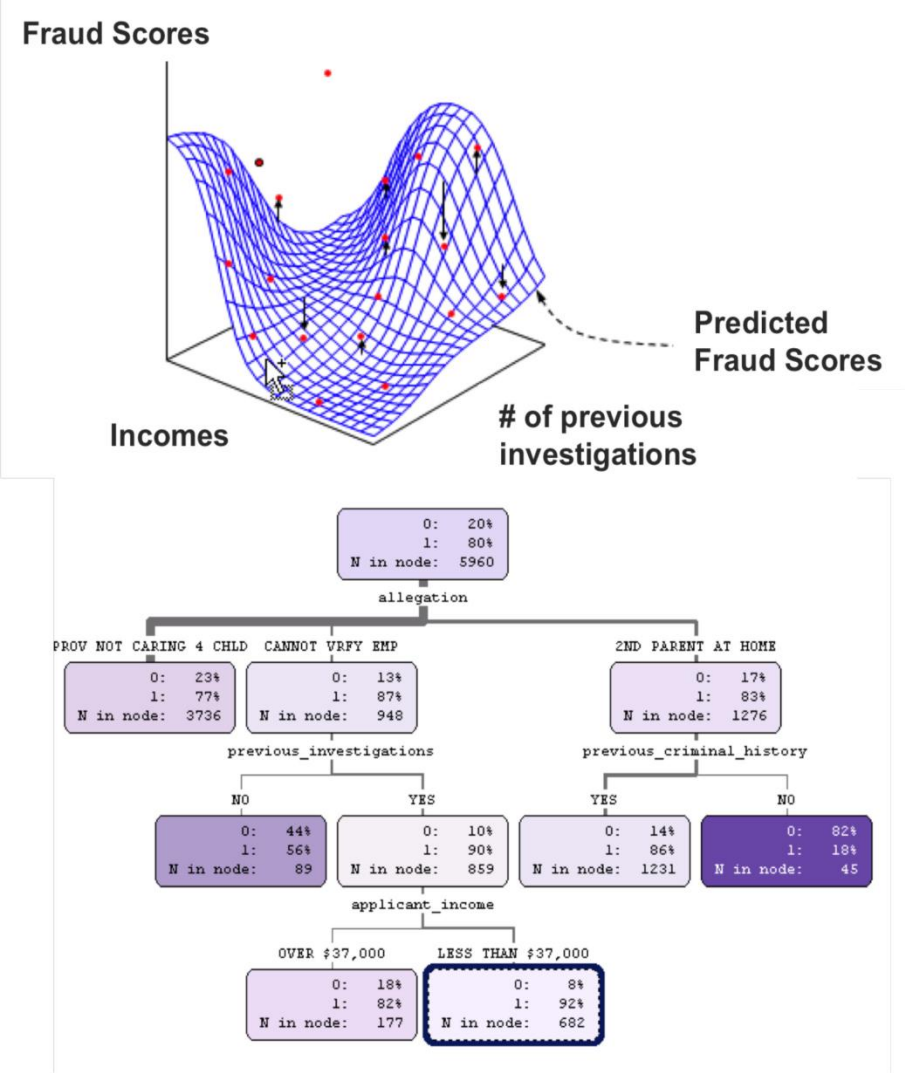

Figure 2: Examples of various predictive models.

Social Network Analysis and Multi-Entity Fraud

Model relationships between entities to uncover abnormal claims patterns.

Social network analysis has proven effective in identifying organized fraud activities by modeling relationships between entities in claims. Entities may be defined as locations, service providers, members, addresses, telephone numbers – to name just a few. Tools can be tuned to display link frequencies that exceed a programmed threshold. In other words, the extent of connections between certain types of entities may be found to be much greater than would normally be expected, based on statistical analysis of other "networks" of entities.

Large volumes of seemingly unrelated claims can be checked, and then patterns and problems identified. For example, social network analysis might show multiple durable medical equipment providers that are owned by several individuals with similar names and share a large percentage of similar patients. It might reveal multiple claims in a short period of time from related parties, such as members of a single family, or the classic ring associated with doctor or pharmacy shopping.

Such techniques have rarely been employed in the health care arena in the past due to labor-intensive efforts to construct networks manually. However, social network analysis can now be fully automated, with the system continuously updating the interrelated networks with new claims and rescoring for fraud. If a network score indicates fraud or abuse, then this can be used to “red flag” a new claim as it is processed and the system matches it to the network. Investigators can search across the full book-of-business claims in seconds, and turn up visual indications of connections and overlaps among them.

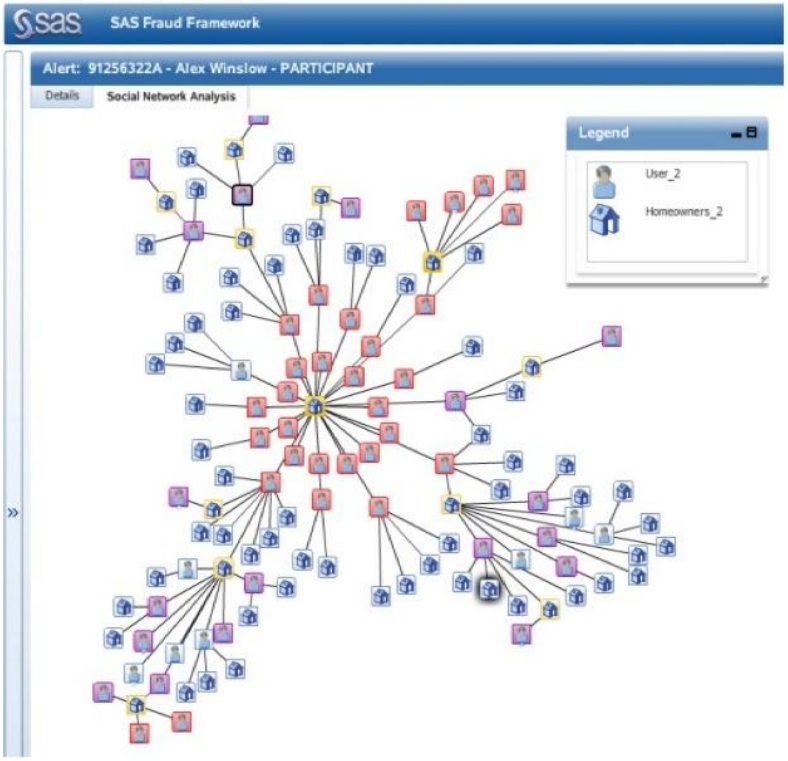

Figure 3: Example of SAS Social Network Analysis indicating fraud or abuse claims with “red flags.”

Risk Scoring, Automated Alert Management/Triage and Integrated Case Management

Dramatically improve investigative efficiency.

With the advent of more sophisticated fraud and abuse detection techniques comes the identification of more leads that require investigation. Perhaps the single, greatest roadblock to the adoption of automated, empirically based detection techniques is the fear that investigators that are already overloaded with leads derived from rules engines and telephone tips simply will not be able to manage the added volume supplied by computational methods. What is often overlooked, however, is the fact that the computational methods also help to eliminate the inefficiencies that have made historical fraud investigation processes so labor-intensive.

To begin, commercially available rules engines have historically focused on identification of suspicious entities (e.g., members, physicians, pharmacies), but have not provided a means by which to prioritize investigations of individual claims associated with those entities. In order to proceed, investigators must look at a complete census or random sample of claims from each suspicious entity, which uncovers two common inefficiencies in the investigative process. First, investigators typically lack user-friendly desktop applications that enable them to query detailed claims data. As a result, investigations are delayed while data is extracted by IT or informatics resources on behalf of investigators. Second, many of the claims that are investigated result in a false-positive finding (i.e., the investigator shows no return for the time invested in preliminary investigation).

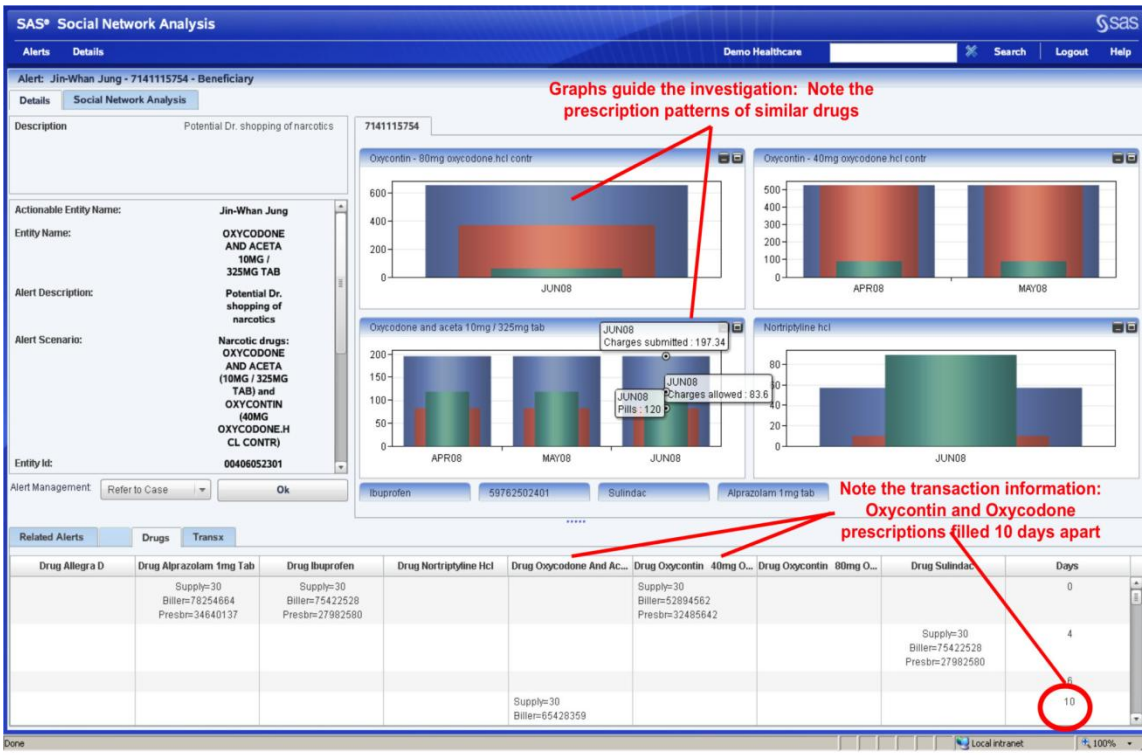

Figure 4: Example of risk scoring and automated alerts.

A state-of-the-art fraud detection solution resolves these issues for investigators. Predictive models automatically attach a fraud risk score to each suspicious claim or lead, and provide details as to why the lead is suspicious. As a result, investigators can immediately prioritize leads for investigation such that false positives are minimized and return on time invested is maximized. Furthermore, detailed claims data supporting the reason for a high fraud or abuse risk score is presented on the desktop at the same time that the lead is surfaced. Investigators also have the ability to drill through and summarize claims data using intuitive, point-and-click interfaces and promote leads to case status so that lead triage time is minimized by 30 to 50 percent. The end result is a greater return with less time consumed in preliminary investigation, thereby opening the door for additional leads to be pursued.

Integrated case management capabilities allow investigators to capture all findings that are relevant to an investigation, including claims data, network diagrams, case notes, surveillance video and any other external structured or non-structured data. Metrics that are known to be key indicators of fraud or abuse are automatically tabulated for comparison at the individual entity or network level. Case workflow is managed (with disposition tracking), which enables a full and complete assessment of investigative workload, efficiency and return on investment. It is this latter capability that promises to resolve the final, major roadblock to full implementation of state-of-the-art fraud investigation techniques in that demonstration of significantly larger ROI serves as the basis for a business case to expand fraud investigation resources.

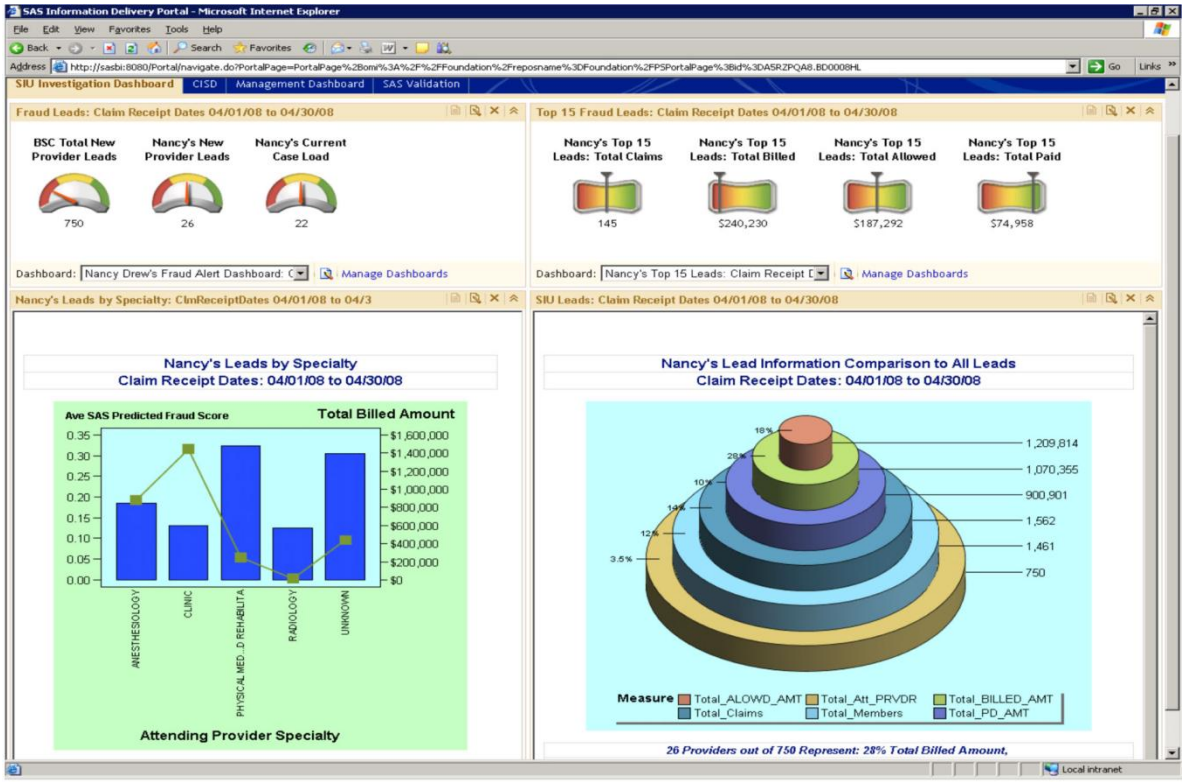

Figure 5: Example of integrated case management capabilities.

CLOSING THOUGHTS

Health care fraud and abuse is an enormous financial burden on a system that is facing unprecedented pressure for cost containment from consumers and legislators. Fraud and abuse contributes directly to administrative costs that inflate health care premiums. And, in the case of for-profit payers, fraud and abuse drains profits from shareholders. The magnitude of potential fraud and abuse savings is such that as more payers recognize and adopt the current state-of-the-art fraud and abuse detection capabilities, those with antiquated fraud management practices will be at a significant competitive disadvantage. Companies that have invested in automated fraud detection systems, especially those that have implemented all or a combination of the above techniques, have been well rewarded for their decisions. One insurer experienced:

- A 100 percent increase in the amount of fraud detected.
- An improved false-positive ratio such that productive leads increased from one in 20 to one in three.
- Decreased time taken by SIU staff to investigate claims by half.

The time is right for health payers to invest in technology to prevent claims fraud and abuse, and stem the current epidemic of financial losses. Technology-based tools to fight insurance fraud can be used individually or in combination to help companies detect and prevent abusive or criminal claim activities. Some fraud detection techniques screen claims during processing and help prevent improper payments. Others involve retrospective analysis of adjudicated claims and help uncover the activities of fraud rings, internal fraud and leakage. Together, these techniques are powerful deterrents for would-be fraudsters who seek to profit at the expense of insurance companies and their honest business partners and customers.

ABOUT SAS

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions delivered within an integrated framework, SAS helps customers at more than 45,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW®.

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Name:	Julie Malida
Enterprise:	SAS institute
Address:	SAS Campus Drive
City, State ZIP:	Cary, NC, 27513
Work Phone:	+1 919 677 8000
Fax:	
E-mail:	Julie.Malida@sas.com
Web:	www.sas.com