
Introducing Identity Resolution

A New Approach to Workers' Compensation Fraud

Charles Clendenen

Abstract

Workers' compensation fraud is a serious problem for the various workers' compensation systems administered by states nationwide. The Ohio Bureau of Workers' Compensation, for example, estimates that they pay as much as \$320 million annually in fraudulent claims (2008). This paper briefly reviews the three major classes of workers' compensation fraud, i.e., fraud committed by medical providers, by employees making claims, and by employers who avoid paying premiums. The article then introduces a new technology, called "identity resolution," that is being applied to the workers' compensation employer fraud problem. Next, the software and how it works is described, followed by a discussion of the return on investment (ROI) that agencies may expect to derive through better detection of employer fraud.

* Director of Professional Services, Infoglide, Inc., Austin, TX.
Email: cclendenen@infoglide.com

If there is one topic that unifies all parties involved in workers' compensation, that topic is the desire to eliminate fraud. Whether it is created by the employer/insurance company or the employee, there is no place for fraud in the system and legitimate efforts to eliminate it are worthwhile.

— Leonard T. Jernigan, Jr., Larson's merging Issues and Trends

Despite volumes of information written every week about workers' compensation fraud committed by employees and medical providers, employers who fraudulently avoid paying premiums may constitute an even more significant threat to the health of state insurance funds. This article discusses three types of workers' compensation fraud and examines a new technology called identity resolution that is being used to improve airline passenger screening. The same technology can be applied to make the process of finding potential employer fraud easier and more cost-effective than current methods.

The Workers' Compensation Problem

The results of a survey by Navigant Consulting conducted for the Bureau of Audits in California highlight the serious problem fraud has become for the various workers' compensation systems administered by states nationwide. The "Workers' Compensation Medical Payment Accuracy Study" published June 17, 2008, does not break out fraud as a separate category, but it estimates that more than 20% of total payments were "errors" (Navigant Consulting, 2008, p. 18). Over \$1 billion in payment errors were processed in a single year in California alone (Navigant Consulting, 2008, p. 26).

The Ohio Bureau of Workers' Compensation estimates that they pay as much as \$320 million annually in fraudulent claims (Ohio Bureau, 2008). Here is their definition:

Fraud is defined as an intentional act or series of acts resulting in payments or benefits to a person or entity that is not entitled

to receive those payments or benefits. Fraud is committed when a person:

- Knowingly receives benefits which he or she is not entitled to receive by law;
- Makes false or misleading statements for the purpose of receiving money or services;
- Enters into a conspiracy to defraud the Ohio State Insurance Fund or self-insuring employer under the Workers' Compensation Act.

Studies conducted by other states, e.g., Texas and Florida, demonstrate similar levels of errors. A small portion of the errors were thought to be administrative mistakes, but these studies made it clear that a significant percentage of errors are potentially the result of fraudulent activity, and anti-fraud efforts in several states are confirming that workers compensation fraud is a significant problem.

While the total aggregate amount of money lost to workers' compensation fraud and abuse of the system may be in dispute, the numbers almost certainly run into the billions nationwide. While many states use technology to address fraud and abuse, a problem this large and costly, involving millions of persons and transactions annually, deserves the assistance of state-of-the-art technology designed for dealing with fraud.

Those involved in bad acts know that their behavior is dishonest, so they try to hide their activities in various ways:

- by making transactions look as normal as possible,
- by obfuscating identity information, and
- by hiding their relationships with other players in the system.

Both traditional and emerging technologies must be applied to stay abreast of the bad actors. No single technology is best for identifying and investigating all types of fraud. The processes of uncovering and verifying indi-

cators of fraud are called *screening* and *targeting*. First, data is screened to identify potentially fraudulent entities and transactions. This is typically an automated process. Next, an investigator who understands the characteristics of true fraud targets (drills down on) the suspicious activity to determine whether fraud is, in fact, taking place. When a domain expert finds likely fraud, emerging technologies can now find even more hidden relationships within previously obscured and obfuscated data, providing additional leads to pursue once the investigator identifies probable fraud.

Types of Workers' Compensation Fraud

Identifying and employing the right software in this struggle requires an understanding of the types of workers' compensation fraud that are burdening the system. There are three types of workers' compensation fraud: medical provider fraud, employee claims fraud, and employer premium fraud (New York State Workers' Compensation Board, 2008).

Medical Fraud

Medical providers can be involved in fraudulent transactions in several ways. They may charge for products and services never provided, or they may charge for more expensive treatments or unnecessary goods or more services than is medically necessary. Fraudulent providers sometimes conduct these activities independently, or at times they conspire with employees being treated. Sometimes attorneys may be involved in fraud rings in collaboration with medical service providers and claimants desiring to make some "free" money.

Since this type of fraud is similar to Medicaid fraud, states and insurers with experience in this area tend to employ the same sort of data mining software (statistical analysis, pattern recognition, neural networks, etc.) to sift through large and complex data sets in order to identify provider fraud. This is an appropriate application of technology for the fraud detection stage. However, not every suspicious transaction is fraud. Once potential fraud is identified, different software capabilities are needed to drill down

and confirm the suspicions raised by data mining technology. While the process of drilling down should focus on individual data records and attributes, it should simultaneously uncover important relationships between other data elements and entities.

For example, if a batch process finds potential fraud, and a domain expert confirms that the activity is probably fraudulent, an investigator may want the software to search the relevant information (attributes) from this newly found information against all the available data. If hidden or difficult-to-find relationships exist, it might indicate that more than one person or entity is involved. In other words, the software casts a wide net to catch potential fraud, and when a data record confirms probable fraud, the software casts a net again in a more targeted fashion to catch more fish of the same type.

Employee Fraud

Employee claims fraud is the type perhaps best known to the general public. There is a constant flow of news stories about individuals who either qualify themselves for workers' compensation benefits by lying about or exaggerating the actual extent and severity of their injury, or else they continue to draw benefits long after they have recovered and are working at another job. Sometimes these individuals are caught when their benefit records are matched with new employment records, but often they are apprehended through the efforts of fraud investigators using traditional detective techniques. Bear in mind that even the most suspicious cases sometimes turn out to be something other than fraud. Technology must always be coupled with human judgment.

Employer Fraud

Employer premium fraud, while less publicized, can involve millions of dollars in unpaid or underpaid premiums and can cause much more damage to the insuring agency. Employer premium fraud can take several forms. In order to avoid paying premiums, a company's owners may illegally classify permanent employees as contractors. Alternately, they may

operate for some time without paying their premiums, and then when the insurer is about to take action, they simply shut down the company on paper and reconstitute it under another name. Companies also use this “going out of business” ploy in cases where their experience (or modification) rating has gone up due to multiple injuries, thereby resulting in higher premiums. By reopening as another company, they can effectively reset their experience rating.

According to New York State’s Workers’ Compensation Board (2008), other employer fraud (or related bad acts) methods include:

- Under-reporting the number of employees,
- Misrepresenting the nature of the work performed by the employee,
- Misrepresenting past loss experience,
- Misrepresenting the company’s ownership,
- Forcing employees to pay premiums that should be paid by the business,
- Discouraging employees from seeking medical treatment,
- Falsely informing an employee that workers’ compensation benefits, are only available if he or she has been employed for six months or more, and
- Getting kickbacks from medical providers for referrals.

Employer fraud is not uncommon, and it can be very difficult to identify without the help of sophisticated software, such as identity resolution solutions. To support all their fraud detection and investigation efforts, workers’ compensation stakeholders need the best technology available. Given the realities of today’s economy, neither states nor employers can afford fraud and abuse of the workers’ compensation insurance systems. Even a modest investment in the fight against fraud likely will result in a significant return.

How Identity Resolution Technology Works

The events of 9/11 accelerated the development of technologies that help find persons intending to cause harm using airplanes. What these would-be terrorists share with other fraudsters is a desire to make their identity difficult or impossible for traditional screening technologies to detect. They do this by modifying portions of the attributes associated with their identity.

Identity resolution software looks at who you are, whom you know, and to what you are connected. It analyzes all the information known about an entity in order to determine whether that entity is a good citizen, customer, organization, or company, or whether instead the entity poses a risk or threat that should be identified and flagged for further investigation. In addition, identity resolution software finds hidden connections that expose fraud networks.

Simply stated, identity resolution technology reveals who's who and who knows whom across multiple, unique data sources containing both structured and unstructured data. An all-encompassing view of internal and external interactions with employees, customers, vendors, and organizations helps to distinguish good from bad, to assess fraud patterns and risk, and to implement and enforce sound policies. Without this information, organizations are much more vulnerable to deception, fraud, and theft.

So how does identity resolution software actually work? First, it aggregates information from multiple existing data stores in order to form a clear, composite depiction of the identity of an individual or other entity (e.g., a company). It then applies sophisticated search algorithms to calculate the distance between search and target attributes. Example attributes for an individual might include name, address, SSN, phone number, and employer's name. Based on the similarity of these multiple attributes, it presents a unified view and it highlights otherwise hidden relationships.

Table 1 shows two different identities for the same person from two different data sources. Note that almost every attribute is different and would

therefore not be identified as the same person by traditional systems, yet to a human being it is quite clear that these two identities are the same person. The similarity search capabilities of identity resolution solutions easily automate the handling of ambiguity.

Table 1
Identity Comparisons across Data Sources

Attribute	Identity #1	Similarity Search Score	Identity #2
First Name	Michelle	95%	Shelly
Last Name	O'Brian	90%	OBryan
Company Name	HARMAN INTL. IND. INC.	95%	HARMAN INTERNATIONAL INDUSTRIES, INC.
Street Address	3550 Twisted Oak Drive	93%	3505 Twisting Oaks
City	Jacksonville	90%	Jackson
State	Florida	100%	FL
Zip Code	35035	91%	35305
Passport ID	MY255909	87%	MJ225090
License Plate	510 B81	82%	SIO 13B
Eye Color	Hazel	90%	Green
DOB	4/11/56	92%	11-4-1956

Identity resolution presents a unified view of individuals with multiple identities. Just as important, comprehensive identity resolution technology uncovers hidden relationships between individuals, whether they are employees, medical providers, or employers.

Applying Identity Resolution to Workers' Compensation Employer Fraud

While identity resolution technologies can be applied to employee and provider fraud, they are particularly effective at uncovering employer premium fraud. Finding companies who are not registered for workers' compensation involves comparing databases where companies are advertising themselves as open for business to lists of businesses registered with state workers' compensation programs. The results can highlight companies who have not registered or are not paying premiums, companies who have changed their name often, and companies involved in hidden contractor/subcontractor relationships. The IRS, other state agencies (e.g., Secretary of State corporation registration, professional licensing, construction permits), and third-party data providers (e.g., Dun & Bradstreet) are good sources of company data.

As stated earlier in this article, some businesses avoid paying workers' compensation by changing their names and identifying data regularly. By analyzing multiple data attributes (company name, owner name, address, phone number, etc.) across multiple state databases, identity resolution software can find matching entities and draw connections between people, places, and things that indicate fraud is likely occurring.

If a contractor hires subcontractors, the hiring contractor is responsible for covering his own workers' compensation, and the subcontractors are supposed to carry their own insurance. Identity resolution software can search multiple data sources to find those who don't have valid workers' compensation (e.g., a licensed HVAC subcontractor falsely claiming the contractor is carrying insurance).

Return on Investment

For organizations that devote budget to fraud detection technology and resources, cost savings as well as revenues generated through increased premium collections more than pay for the investment. In their Annual Fraud Reports to the Legislature, Washington State's Department of Labor

and Industries (L&I) described their Return on Investment (ROI) through vigorous anti-fraud efforts. In 2006 L&I employer audits identified assessments totaling nearly \$21 million; investigations of claimants prevented the loss of over \$15 million; and medical provider reviews resulted in the collection of nearly \$500,000 in improper billings (Washington State Department of Labor and Industries, 2006, p. 6-9). These figures represent a return of \$10.20 for every \$1 spent in anti-fraud efforts.

Washington State attributes these savings to an increase in fraud fighting capability, faster collections, funding for technology advances, and better communications and referrals across the various programs in the department. Additional investment in 2007 brought a major increase in investigation efficiency over 2006, and return on investment achieved a nearly 10 to 1 ratio (ten dollars saved or recovered for each dollar invested).

Besides the monetary savings, 20 fraud cases were referred for prosecution in 2006 and an additional 13 were referred in 2007 (Washington State Department of Labor and Industries, 2007, p. 13). These prosecutions are expected to have a deterrent effect on those who would scam the system.

How to Invest in Anti-Fraud Efforts?

Washington State's investments in applying human capital, technology, and legislation against fraud provide significant benefits to their workers' compensation system. When states evaluate what kinds of investments to make, the answer depends on the type of workers' compensation insurance they have in place. States with exclusive or competitive workers' compensation insurance systems can invest directly by maintaining their own compliance or anti-fraud programs within their workers' compensation departments. States with no investigation or enforcement arm need to pass anti-fraud legislation that mandates oversight to verify that private insurance carriers comply with anti-fraud insurance laws.

In either case, adding identity resolution can significantly increase investigator productivity by prioritizing the potential fraud cases that are detected and can provide significant return on investment by uncovering

fraud, preventing loss, and aiding in collection from or the prosecution of fraudsters. In short, there is ample and convincing evidence that anti-fraud investments (increased staff, more effective technology, and better laws on the books) pay for themselves many times over.

Conclusion

Data mining is still an excellent way of screening large and complex data stores to identify patterns that indicate potential fraud. Newer identity resolution and relationship detection software, however, is emerging as a method of enhanced data screening and discovery of suspicious relationships that reflect fraudulent activity. And identity resolution, coupled with relationship detection and visualization capabilities, is a promising new technology for investigators to use for drilling down on information relating to individuals and rings suspected of fraud.

References

- Navigant Consulting. (2008). California Department of Insurance Workers' Compensation Medical Payment Accuracy Study. Retrieved December 20, 2008, from State of California website at: http://www.insurance.ca.gov/0300-fraud/0100-fraud-division-overview/0500-fraud-division-programs/workers-comp-fraud/upload/Navigant_Medical_Payment_Report.pdf
- New York State Workers' Compensation Board. (2008). Types of Fraud Investigated by the Office of the Inspector General. Retrieved December 20, 2008, from State of New York website at: <http://www.wcb.state.ny.us/content/main/fraud/WhatIsFraud.jsp>
- Ohio Bureau of Workers' Compensation. (2008). Fraud and Workers' Compensation. Retrieved December 20, 2008, from Ohio Bureau website at: <http://www.ohiobwc.com/basics/guidedtour/general-info/generalinfo7.asp>

Washington State Department of Labor and Industries. (2006). *2006 Annual Fraud Report to the Legislature: Targeting Fraud and Abuse – Washington State’s Workers’ Compensation System*. Retrieved December 20, 2008, from State of Washington website at:
<http://www.lni.wa.gov/IPUB/262-276-000.pdf>

Washington State Department of Labor and Industries. (2007). *2007 Annual Fraud Report to the Legislature: Targeting Fraud and Abuse In Washington State’s Workers’ Compensation System*. Retrieved December 20, 2008, from State of Washington website at:
<http://www.lni.wa.gov/IPUB/262-280-000.pdf>

Charles Clendenen has over ten years of private and government sector experience in technology, testing, project management, and delivery of professional services. Mr. Clendenen’s business career was preceded by over twenty years in security and military intelligence for the U.S. Army. He has spent over eight years at Infoglide Software, primarily in support of Homeland Security and state government identity resolution projects as a solutions manager and technical lead. He has previously held positions at Pervasive Software and Transactive Corporation.

Editor’s note: As sought under the procedures of this Journal, the author has disclosed that his employer, Infoglide Software sells a product that might be of interest to readers in the field of workers’ compensation claims.