# Speed to Detection with Advanced Analytics - Fraud Reduction Strategies for 2014

John Standish
Chief Marketing Officer

Infinilytics, Inc.

**Abstract**: Despite a large defense shield, growing numbers of insurance executives at the decision-making levels — inside and outside the anti-fraud ranks — are frustrated that fraud persists as a costly epidemic. Optimizing speed to detection is a corporate mindset that synchronizes all layers of insurer personnel into anti-fraud advocates who are well-trained about this crime, personally motivated and follow internal processes that allow open lines of communication about fraud leads, needed process improvements and action solutions. Reaching this goal must start with an honest discussion about technology and other best practices. A major problem is that too many insurers use outmoded methods of fraud detection. These methods have little impact on modern, sophisticated fraud rings that are a significant source of money outflow. Advanced analytics ranks among today's most transformative best practices for increasing speed to detection and allowing better-informed decision making. Big data is another concept increasingly being discussed. Insurers also must reduce reliance on the ineffective pay-and-chase mode of combating fraud. And they must commit to taking on the difficult and expensive cases such as complex organized crime rings, which are growing in number and ability to steal insurance money.

**Speed to detection: a progressive and strategic concept using advanced anti-fraud analytics**
**Insurers must transform strategies for combating complex crime rings**

By John Standish

The recent natural disasters in Oklahoma and New Jersey, and the wildfire season in the western United States, have a lot in common when one thinks both of insurance risk — plus the intended and unintended consequences of these events.

The insurance industry knows natural disasters will happen. The industry thus creates and follows protocols and response plans. For the most part, the industry and public-safety officials handle the crisis, and restore calm and order in our communities.

The insurance industry knows these events will occur, and planning is generally pretty solid per the axiom, "If it's predictable, it's preventable."

But in the world of insurance fraud, many sectors of the insurance industry seem to lack the same energy to mitigate this crime. Using the same acumen gained from restoring order after disasters, the key is to apply the same proven strategies of history, response, performance and mitigation of future risks. This approach will better help combat insurance fraud with equal success.

The modern strategy of "speed to detection" is a uniting principal and operating strategy for mitigating the epidemic of fraudulent claims.

Optimizing speed to detection involves synchronizing all layers of insurer personnel into informed, enterprise-wide fraud fighters. They are well-trained to spot warning signs of this

crime, personally motivated, and encouraged to follow internal processes that allow open lines of communication about fraud leads, needed process improvements and action solutions.

Bogus claims claims thus can be discovered and mitigated faster. Quick detection also is an intimidating deterrent that can convince more fraudsters to avoid trying to breach that insurer. The risk of arrest and conviction is too high, and odds of financial reward are too low.

Speed to detection is a timely precept: Insurers today are confronting a persistent crime that is morphing, in many respects, to higher levels of sophistication and ability to steal insurance money.

Insurance fraud harms law-abiding consumers (higher premiums), aids the underground economy, facilitates other illegal enterprises such as trade-based money-laundering, and poses a public-safety threat (e.g., staged automobile collisions, arson, murder for life insurance, needless medical procedures).

Conservatively, fraud steals $80 billion a year across all lines of insurance.[1] Some estimates rate the annual losses much higher.

And the problem is growing. Questionable property-casualty claims in the U.S. have increased 27 percent in 2012 over 2010, the National Insurance Crime Bureau (NICB) says in an analysis of its database of claims released in May.

That reflects 91,652 questionable claims in 2010 compared to 116,171 claims in 2012.[2]

Similarly, most consumer research reveals a disturbing public cynicism about this crime, and even a backslide toward higher consumer tolerance of fraud.[3]

Confronting this epidemic is a large network of organizations dedicated to minimizing fraud as a virulent national threat.

Insurance companies have teams of experts (the Special Investigation Unit, or SIU) trained to deal with suspicious claims.

State law-enforcement agencies have created specialized departments and bureaus dedicated to thwarting this crime.

State insurance departments have strengthened their processes for identifying, investigating and reporting suspicious claims for potential prosecution.

States also have enacted numerous fraud laws and regulations that further strengthen enforcement. More are being added or bolstered every year.

At first glance, these processes appear sound, prudent and presumably effective. A lot of money, personnel and effort have been thrown at insurance fraud. Shouldn't schemes be going down instead of up? Or at minimum, leveling off?

Many of the following observations are guided by my 32 years of combating insurance fraud, including several years as a Bureau Chief, and one year as the Division Chief with the nation's largest anti-fraud unit, the California Department of Insurance, Fraud Division. Some academic backup also is cited for added information.

Despite the large defense shield, growing numbers of insurance executives at the decision-making levels — inside and outside the anti-fraud ranks — are frustrated about how fraud persists as a costly national epidemic.

To illustrate: In recent years, I have provided consulting and analysis and review of first- party bad-faith cases involving fraud, the actions of SIUs in a claim or series of claims, and expertise for qui tam civil actions by insurance companies.

In these many interactions with insurance executives, anti-fraud directors and other colleagues throughout the industry, the frustrated question they ask most often about fraud is:

"Why do we keep throwing money at a crime that never seems to go away?" Typically they some offer two reasons why fraud remains so vexing and persistent:

"The insurance system invites fraud." Indeed, our insurance system is one of the best in the world. But the most skillful fraudsters effectively exploit weaknesses when the system is not synchronized and calibrated among partners to create a hardened shield.

"We need the best team to investigate these crimes." Insurance companies and government entities are constantly working to create an elusive Dream Team for investigations. Key ingredients of team members are passion, creativity, and ability to wade through a series of complex conspiracies either to deny a claim, or have an offender arrested and prosecuted.

Many insurers are frustrated because qualified people with the acumen to investigate fraud is hard to come by. Time after time, when insurance carriers lose bad-faith lawsuits involving the SIU and fraud, some of the common denominators are training, unqualified people and bad leadership decisions.

An important reason fraud appears to keep rising is that insurance companies and regulators are slow to recognize the value and impact of anti-fraud technology leveraged with best business practices.

The anti-fraud community needs to rethink its strategies, and examine ways to identify problems and risks before they become crimes.

Resources should be synchronized to optimize speed to detection.
This requires insurers to have their anti-fraud operations well-aligned with their internal corporate structure, strategies and practices — and with external partners such as state fraud

bureaus, law enforcement and NICB.
Reaching this goal must start with an honest discussion about technology and other best

practices. A major problem is that too many insurers use outmoded methods of fraud detection. These methods have little impact on modern, sophisticated fraud rings that are a significant source of money outflow.

Meanwhile, insurance fraud is evolving and organized crime increasingly is infiltrating fraud. Such rings have been around for years, but their sheer number and growing sophistication are changing the criminal landscape. Many insurers aren't equipped to counter this new breed of criminal, especially using indicators.

Recently, I gave a presentation at the Insurance Fraud Management Symposium (IFM). This is the largest annual conference of insurer anti-fraud directors, executives and other personnel. [4]
The presentation covered a major criminal investigation and prosecution involving a staged-

accident ring in Southern California.
This case illustrates two frequent insurer vulnerabilities: a) over-reliance on weak fraud

indicators that allowed fraudsters to penetrate the insurer's anti-fraud defenses relatively easily; and b) how vulnerable insurers become when they compromise their business processes by speeding up claims payouts by compromising vigilance.

The leader of this criminal enterprise joined me in the presentation. He was under court order to assist the California Division of Insurance in public education after his conviction.

He related how he ran the operation, who he involved, and how and why he targeted specific insurance companies with bogus injury claims from the setup collisions.

He made a chilling point: "You will never win the war on fraud." He urged insurers to avoid over-reliance on the so-called "indicators" they use to identify fraudulent claims. Indicators are a relatively basic investigative tool. Insurers look for specific actions or behaviors that are red flags of possible fraud during the claims process. With staged accidents, for example, indicators might include flags such as multiple people in both vehicles, expensive treatment at the same clinic, and similar last names to suggest a possible family fraud ring.

This ringleader knew the indicators well, probably better than some claims staff. Thus he could rig his crashes and phony claims to easily avoid being detected by common flags. Just as important, he also relied on inexperienced and untrained claims representatives to give in and pay claims with little scrutiny.

“It is a game of poker: Who is going to bluff the best, and who will stay in the game with a winning hand?” he warned.

In similarly illustrative case, Greg Foshee was educated, articulate and knew the insurance-claims system well. He should have. Foshee was a claims representative for one of the nation’s largest property-casualty insurers. He saw large profit potential when his supervisor ordered him to “just process the claims.”

So Foshee went to the “dark side.” He started staging vehicle accidents and then helped process the ensuing bogus injury claims without insurer scrutiny.

He staged more than 82 vehicle collisions that stole $1 million worth of insurance money. During questioning after his arrest, Foshee said his supervisors told him: “Don’t ask too many questions, just get the claims off your desk.”

Foshee used multiple individuals with multiple valid drivers licenses from several states. He kept the operation simple to avoid detection. He had only 13 ring members, with just three cohorts working full time and controlling the group.

Nor did Foshee involve attorneys and physicians. They would have slowed the claims, and he would have had to split the ill-gotten insurance money with them.

He made smaller claims just for vehicle damage and minor medical treatments in order to stay under insurer radars. The treatments usually consisted of an emergency-room visit for subjective injuries such as whiplash that are typically associated with minor traffic accidents.

Foshee also knew that if his ring members went to emergency rooms too often in a given city, someone might notice and start asking questions. So instead he created false medical bills and treatment reports using letterhead and forms stolen from the hospital.

If the targeted insurance companies had simply called the hospitals to verify patient information, they would have discovered that the so-called patients were never treated there. This would have confirmed that the treatment reports and bills were false.

Foshee averaged $10,000-12,000 income per staged accident, and went undetected for several years. He knew how the claims process worked, and how to avoid scrutiny and detection.

The California Highway Patrol’s Investigations Unit completed the investigation in 1988. Foshee was convicted of insurance fraud, conspiracy, grand theft, and was sentenced to several years in state prison.

Let’s think about this for a minute ... These aren’t isolated cases. Over the last 30 years, large segments of the insurance industry, law enforcement and other government agencies have relied heavily on old-fashioned indicators of false claims, and similar basic tools. These indicators have

been identified, written, promulgated, and used in the daily business of receiving and closing insurance claims.

Reality check, please?

The crime rings knew the insurers' fraud indicators, and avoided them. The insurers also compromised their internal anti-fraud processes to turn around claims quickly.

Many other organized fraud groups and bold criminal entrepreneurs these are operating daily, skillfully compromising the insurer claims systems. Collectively, they likely steal millions of dollars everyday. Whether detected or undetected, usually it is too late to recoup the stolen money.

**Rethinking the fraud fight**

If speed to detection is to move from an energizing concept to transformative anti-fraud practice, fraud fighters must step out of the indicator box and rethink their entire approach to combating modern, emerging threats such as complex and organized crime rings.

Some insurers just seem to be going through the motions of fighting fraud, indicators and all. But the more progressive insurers are transforming their internal cultures and business practices to create a coordinated, enterprise-wide response to this crime.

They are taking the fight more directly to the criminal underworld instead of waiting for the underworld to come to them. As a result, these insurers also far more resistant to schemers of all kinds.

Insurance companies and government agencies need the ability to change direction quickly to address emerging fraud schemes, trends and problems. Nimbleness is a key attribute of sophisticated fraudsters. It also should be a core trait of every insurer's speed-to-detection process.

The goal is not to eliminate fraud indicators or other basic tools. These tools may play a role in the overall mix of anti-fraud business processes and strategies each insurer custom fits for its own anti-fraud challenges.

Several strategic best practices can help optimize speed to detection.

**Advancing analytics**

Advanced analytics rank among today's most transformative best practices for increasing speed to detection and allowing better-informed decision making.[5]

Analytics involves the discovery and practical use of meaningful patterns of anti-fraud data. Properly marshaled, advanced analytics can quickly move insurers miles beyond indicators. Analytics can reduce the ineffective pay-and-chase mindset of many insurer detection processes.

Analytics also can put insurers quickly on the offensive, and thus dramatically increasing speed to detection.

Advanced analytics tools come in many flavors. Each organization must customize an analytics strategy to its unique challenges. Rarely is there one off-the-shelf software solution. Analytics solutions increasingly are being adopted by some insurers. Among the solutions that are gaining momentum:

Predictive analytics. Allows insurers to uncover suspicious activity in close to real time, and even to forecast the likelihood of potentially fraudulent behaviors.

Text analysis. Insurers can ferret out previously inaccessible data such as an adjuster's field notes — even handwritten notes.

Social network (link) analysis. Helps an insurer examine relationships among organizations, people and transactions to discover suspiciously related claims that appear unrelated on the surface.

Social media analysis. More insurers recently have begun mining social media for clues. A workers compensation insurer, for example, might uncover a supposedly disabled worker posting photos of his Hawaiian surfing vacation on his Facebook page.

But analytics alone — whether advanced or more basic — cannot reverse the tide of fraud. Analytics must be supported by other best practices and processes.

Some insurers and smaller regulatory agencies believe the cost of advanced analytics platforms is too high, or that they do not have the data to support such robust systems.

But analytics can be affordable by starting small (don't try to boil the ocean), and strategically planning to gradually layer in advanced analytics into the business process and technology platform. Start small, and build upon the new platform incrementally, first addressing immediate business needs and problems.

**Marshall big data**

Mobilizing big data is gaining wider attention in anti-fraud circles. Insurers are sitting on troves of data, hard and soft. Much is never accessed for fraud-fighting. Insurers can dramatically increase their anti-fraud assertiveness by insightfully accessing, analyzing and mobilizing their large volumes of untapped data.

But the terabytes and even petabytes can overwhelm an insurer's analytical capabilities.

Insurers must invest in analytic expertise to retrieve, filter and use big data properly. Insurers also must know what questions to ask when mining for big data. This information will be more focused and useful, and avoid the confusion and fuzzy results that too much data can impose.

**Limit pay and chase**

Insurers must re-evaluate their reliance the ineffective "pay-and-chase" model that drives anti-fraud-strategies of so many insurers. Using this model, insurers routinely pay claims and then investigate afterward.

But the money is gone by then, and the trail is growing cold. It is rare for an insurance company, self-insured or government program to recover much or any stolen money. In fact, usually no money is recovered.

This is especially true of the larger, complex fraud rings that often operate internationally. They are adept at trade-based laundering of stolen insurance money through shell corporations.

Some insurance rings are learning from criminal brethren such as drug cartels in Mexico and South America. They are effectively laundering stolen money (e.g., proceeds from human trafficking, firearms and narcotics). They wash the money through sophisticated shell companies and corporations involved in global commerce. The money is difficult, if not impossible, to trace and recover.

In the public sector, Medicare once was the poster child for ineffective pay-and-chase practices. But the federal health program for seniors is replacing that approach in part by installing predictive analytics to uncover more false claims before payment.

**Take on difficult cases**

Simply going after safe, low-level frauds (i.e., low-hanging fruit such as an inflated claim from a home burglary) might look good on the anti-fraud unit's statistics reports.

But this also may ignore the largest fraud problems and sources of claims-money outflow such as modern rings that steal safely and efficiently.

They often are organized like a classic cell network. Ring members do not know each other, nor do they know all activities in the enterprise. But advanced analytics can expose these complex groups and their crimes much faster and more efficiently.

Insurers must commit to taking on the difficult higher-dollar cases such organized crime rings, even if it entails considerable cost and personnel. This is essential to diminishing what for many insurers is a significant source of false claims payouts.

**Collaboration**

Better collaboration is essential to turning the corner on America's fraud epidemic. This collaboration must include all stakeholder organizations and personnel.

**Internal**. Collaboration within an organization should be an enterprise-wide endeavor and operational commitment. For example, a) agents and brokers must speak with the claims staff; b) claims staff communicates with the SIU team about suspicious claims; and c) employees at all levels must be encouraged to speak up and identify vulnerabilities, process breakdowns and needed solutions.

To underscore this point, visit another statement the fraud-ring member said at the IFM conference:

"We know when the insurance company will pay based on the actions and interaction with an inexperienced, and not properly trained, claims representative. And we also know which companies pay claims easily."

**External.** Insurers must retain open lines of communication with state fraud bureaus, local law enforcement, state attorneys general, the FBI and other stakeholders.

Insurers in different lines of insurance also must collaborate. Auto, workers compensation and health insurers, for example, may find synergy by comparing best practices and exchanging case leads that may uncover hidden crimes.

Insurers in the public and private sectors also must better collaborate for the same reasons. Many organized crime rings, for example, defraud numerous insurance programs. A large Armenian crime ring in California, for instance, staged car crashes against auto insurers and also bilked Medicare. If public and private insurance program share case leads, they can dramatically increase the joint knowledge base needed to more speedily break down that ring.

One promising collaborative effort is the new Fraud Prevention Partnership. It was formally announced last July by HHS Secretary Kathleen Sebelius and U.S. Attorney General Eric Holder. 6

Medicare, private health insurers, automobile insurers and others are formalizing closer lines of cooperation. The partnership is building up its operating structure, and partnership members are beginning to share fruitful case leads. It could become a model for collaborative techniques.

**The payoff**

Marshaling analytics and big data with current rules and indicators into a seamless and unified anti-fraud effort creates an expansive world of possibilities.

Imagine the ability to search a billion rows of data and derive incisive answers to complex questions in seconds.

Imagine being able to comb through huge numbers of claim files quickly.

Imagine more-quickly linking numerous ring members and entities acting in well-disguised concert. These suspects likely could not be detected with sole or even primary reliance on basic methods such as fraud indicators.

Ultimately, imagine analyzing entire caseloads faster and more completely, thus addressing the largest fraud problems and cost drivers in any of an insurer's coverage territories.

**Conclusion**

Insurance companies are not in the anti-fraud business. They are in the business of managing a risk pool, mitigating those risks and returning a fair profit. Government law-enforcement agencies are specifically charged with preventing crime and disorder.

To prevent fraud, all involved organizations must scrutinize their systems with a fresh view and openness to evaluating how to better combat this crime.

Advanced analytics, coupled with sound business practices and preventive measures, will yield better anti-fraud results. For insurance swindlers, speed to detection should mean speed to jail.

About the author: John Standish most recently was Division Chief of the California Department of Insurance, Fraud Division. He retired after 32 years with the California Highway Patrol and Department of Insurance. Standish is now the Chief Marketing Officer for Infinilytics, Inc. (www.infinilytics.com), and consults for litigation involving fraud, SIU operations, and qui tam actions.

[1] Coalition Against Insurance Fraud, estimate of annual fraud losses

[2] *U.S. Questionable Claims Report,* National Insurance Crime Bureau, May 16, 2013 https://www.nicb.org/newsroom/news-releases/u-s--questionable-claims-report

[3] *Four Faces of Insurance Fraud,* Coalition Against Fraud, 2007; Poor Service Leads to Fraudulent Claims, Accenture consumer survey, 2010 http://newsroom.accenture.com/article_display.cfm? article_id=5061

[4] *An Insider's Perspective on Automobile Insurance Fraud - Why It Is So Easy to Steal From Insurance Companies, and What To Do About It. White Paper by SAS, 2013 http://www.sas.com/reg/wp/corp/59146*

[5] *Competing on Analytics, The New Science of Winning.* Thomas H. Davenport and Jeanne Harris, Harvard Business School Press. 2007.

[6] *New Anti-Fraud Partnership is a Force Multiplier, news release,* Coalition Against Insurance Fraud, July 25, 2012. http://www.insurancefraud.org/news-release-detail.htm?recid=3162#.UcDJshYch0g