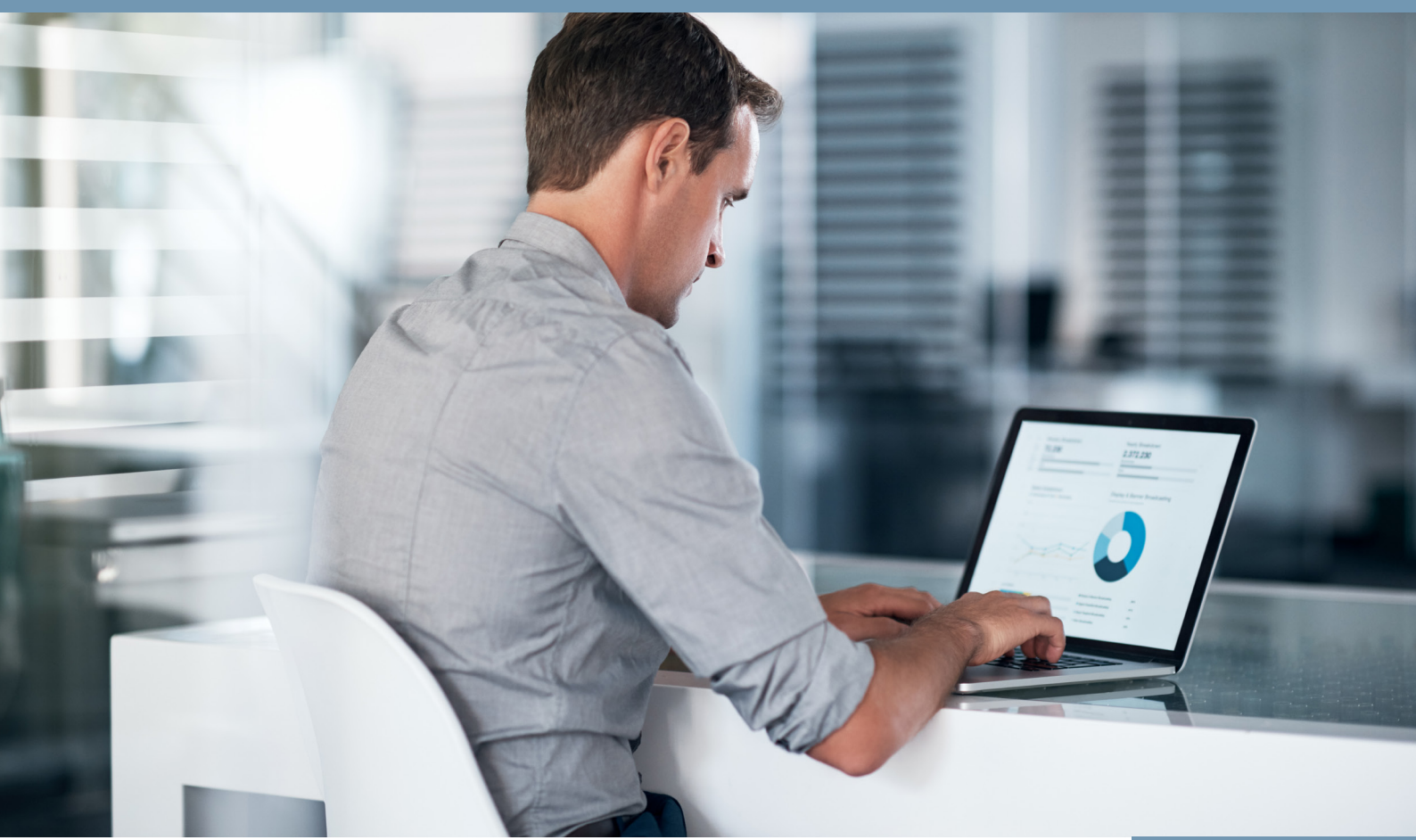
WHITE PAPER

Fighting Insurance Application Fraud

Early detection of agent gaming, customer gaming and the potential for future claims fraud



sas
THE POWER TO KNOW.

Contents

A tempting opportunity

A veteran fraudster, Bill was aware that insurance claims could be a good source of new revenue. It would be so easy to find Social Security numbers of people who wouldn't notice if policies were taken out in their names – like children or dead people…

Nearing the end of the quarter, Jane was in a bind. Sales had been slow, and she was at risk of not making quota. It would be so easy to open new policies with existing clients before the end of the quarter (they wouldn't know), then cancel the policies at the start of the next quarter…

At 22, Bob was moving into his own flat. When he looked into auto insurance quotes for himself as principal driver, parking on the street downtown, the premium spike shocked him. It would be so easy to just list Dad as the primary driver, say the car lives at Dad's rural address, and reduce the cost…

As more applications and policy originations take place through digital devices and the internet, fraudsters gain the access and anonymity on which they thrive. Insurers can't easily verify the applicants and the risk that they are looking to write. The digital channel opens new opportunities to:

- Get insurance policies for fictitious beneficiaries.
- Open and cancel policies for agent benefit.
- Modify application information to reduce premiums.

Ironically, initiatives designed to harden privacy and security have in some ways made application fraud easier or simply caused fraudsters to move to other avenues. For example, the randomization of the Social Security number issuing process in the US in 2011 made it more difficult to compare numbers with dates of birth and locations of insurants. In other words, it's easier for fraudulent applications to get by. Furthermore, insurance agents and brokers understand how to "game" the application system and process; they know it intimately.

On the other hand, the use of digital channels creates new data about device fingerprint, IP address, geolocation and more – data that can be folded into analysis to build a richer, holistic view into the validity of an application.

Overview of insurance application fraud

The initiation of a relationship is the first opportunity to detect and/or prevent fraud, so it makes sense to have strong tools and procedures during the application process. Combating insurance application and underwriting fraud entails four types of activities:

- Verify the identity of the individual making the application.
- Identify the potential for future claims fraud at the point of application.
- Spot customers gaming the system to their advantage when using direct channels.
- Detect insurance agents who are filing nefarious applications in broker channels.

When a fraudulent application escapes detection, the fraudster gains financially while the insurer takes on a new policy with a skewed picture of the underlying realities. Either outcome is unacceptable to insurers – and it isn't inevitable. Here are some effective defense strategies powered by analytics.

Verify identity at the point of digital application

This is more than a background check. It is about deep due diligence to validate the identity of an individual using a digital device:

- **Identity verification** confirms that an applicant's details match historical records, such as from credit bureaus and other sources. This is the process of tying a user account to a verifiable real-world identity.
- **Identity authentication**, which is not universally used, ensures that applicants are who they claim to be – typically by gathering information that cannot be easily forged or faked, such as a secret that would only be known to that person. Smart authentication relies on multiple data sources and matches the transaction's risk level.
- **Device verification** analyzes and compares device information to past experiences and the information provided by the person generating the application. Was this device used in the past, and was it associated with the same customer, physical address, agent, etc.?

Organizations have masses of data – internal and external – that can be used to determine the authenticity of an application and the individual behind it (if there even is an actual person behind it). Here are some leading approaches:

- **Monitor application data**. Building profiles of each data element in an application can help spot the reuse of information across multiple identities or the reuse of the same laptops to create and manage multiple identities that are otherwise unrelated.
- **Assess past experience**. What is the insurer's experience with applications that included the same data element, such as the same device ID, address or SSN? Were any declined? Were accounts closed for cause or fraud? Negative information may prompt further due diligence to understand the relationships between accounts and applicants.
- **Find "proof of life."** Many fake identities don't have records we would associate with a real person, such as driver's license, voter registration or property ownership. Lack of well-rounded identity details can be a strong red flag to a fraudulent applicant.
- **Analyze the network**. Network analysis plays a big role in understanding the connections (or lack of a connections) among applicants, devices, policies and application data. Visualizations of these links can be very useful both in assessing applications and conducting investigations.

Application fraud has several different flavors, but all involve the submission of false or manipulated information to influence policy decisions in someone's favor.

Insurers who distribute their policies through agents and brokers face additional threat of agent gaming, manipulating the underwriting data for the agent's benefit.

Any organization doing business on the internet faces the risk of application fraud, but also new opportunities to detect and prevent application fraud and the future losses it brings.

Prevent future claims fraud at the point of application

Everybody in the insurance industry is well aware of the staggering loss to claims fraud. The Coalition Against Insurance Fraud estimates that claims fraud represents about $80 billion a year in the US alone. The Insurance Information Institute puts that figure at $32 billion a year just in the property and casualty area.

This is a global phenomenon. For example, undetected fraud costs insurers in the UK an estimated £3 billion a year, according to the Association of British Insurers. Suspected losses are €4 billion a year in Germany,[1] $2 billion in Australia[2] and $4.5 billion in Korea.[3] Insurance boards in other countries estimate that between 10 percent and 32 percent of claims are fraudulent, at a high cost to insurers and their honest customers.

What if you could stop those losses before they ever have a chance to get started? What if you could use intelligence gained from the claims detection process to better understand new applications? What if you could tag applications that show potential for future claims fraud and send those directly to investigative teams?

Insurers around the world are subject to different regulatory and cultural standards regarding protocol for this, but at its core it's about learning from experience and, through analytics, bringing that knowledge to the front of the insurance policy life cycle.

Let's look at a basic example. Figure 1 shows a very simple network that includes a claim alert on Aug. 8. Social network analysis shows some connected entities – vehicles, policies and people – as well as other claims associated with that claim alert.

By applying high-scoring claims network entities as filters for new business applications, you can spot potential problems. When a new application matches elements of a high-scoring network, the insurer can choose to handle that application differently and stop that high-scoring network from expanding.

Connections can be established not just through people or vehicles (addresses, telephone numbers, VINs, etc.), but through any number of attributes, such as IP addresses, devices, bank accounts, repair shops and other providers. Enrich the discovery by applying key scenarios learned from the claims process. What did fraud look like in the past, and does this application match into it? Insurers around the globe who are doing this are reaping results.

And through machine learning, a form of artificial intelligence, new information gained through analysis can be fed back into models for continuous improvement.

Preventing customer application fraud starts with validating the identity of an individual. Are they really who they say they are? For insurers who really want to crack down on fraud, it's also about applying analytics to spot aberrant behaviors, suspicious connections and the earliest signs of potential future fraud.

Most insurers will want to make use of the intelligence and analytics built up in the claims process to better understand new business and the underwriting process.

1 Source: German Insurance Association (GDV)

2 Source: Insurance Fraud Bureau of Australia (IFBA)

3 Source: Korean Financial Supervisory Service (FSS)

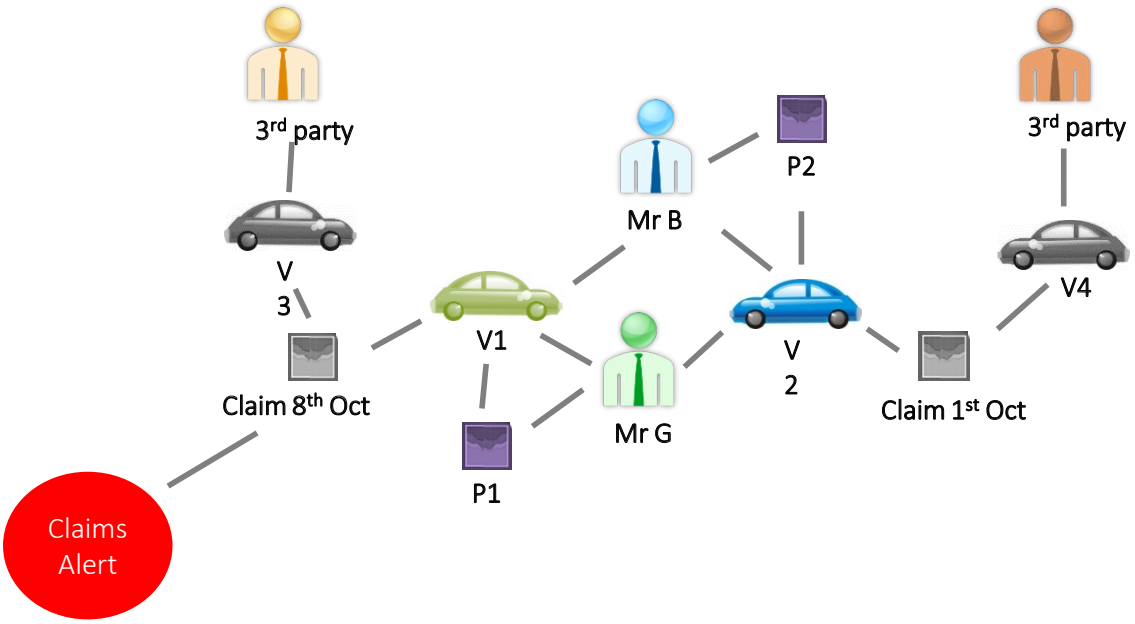


Figure 1. Network link analysis: Connect the dots by seeing links between prior claims alerts and new applications.

Identify agent gaming

Insurance agents, both tied to an insurance company or independent, have a lot of options for gaming the system for personal benefit. For example:

- **Lapping** – Steal premiums and cover them up by crediting a fake customer account with another customer's premium.
- **Skimming** – Steal premiums before the payments are credited into the customers' accounts maintained by the insurer.
- **Fictitious policies** – "Invest" your own money to pay premiums on policies that earn incentives and bonuses, or sell policies to customers but don't file the policies with the carriers.
- **Forgery** – Forge policyholders' signatures to steal premiums and cash values of insurance policies.
- **Churning** – Persuade customers to terminate their existing policies and buy new ones, often with unwanted and unneeded coverages, to earn extra commissions.

As a result of these tactics, the insured will pay less than the real risk premium. Claims frequency and severity will be higher than expected. Future ratemaking reviews will be based on poor data that does not reflect the real book of business. All for business the insurance company may not have wanted in the first place.

A multipronged defense against agent gaming

A number of analytics techniques can lead you to agents who might warrant a closer look. A well-rounded fraud solution will capitalize on multiple techniques to deliver a risk score for agents, showing high-scoring agents and the evidence that led to those scores.

Agency metrics/scenarios fuel machine learning for this purpose. Scenarios learned from past SAS experience are used as inputs for unsupervised or supervised machine learning, where the algorithm finds and learns from patterns in the data. Unlike hypothesis-driven analysis, machine learning can uncover what you didn't know to look for. Machine learning might use scenarios related to address discrepancies, claims, discounts, hidden drivers, fictitious policies, money handling, rating and more.

Peer grouping clusters agents based on attributes that make good comparison groups. You could group agents by geography, urban or rural, book of business, career level, specializations and more, to assess their activity relative to peers and spot differences.

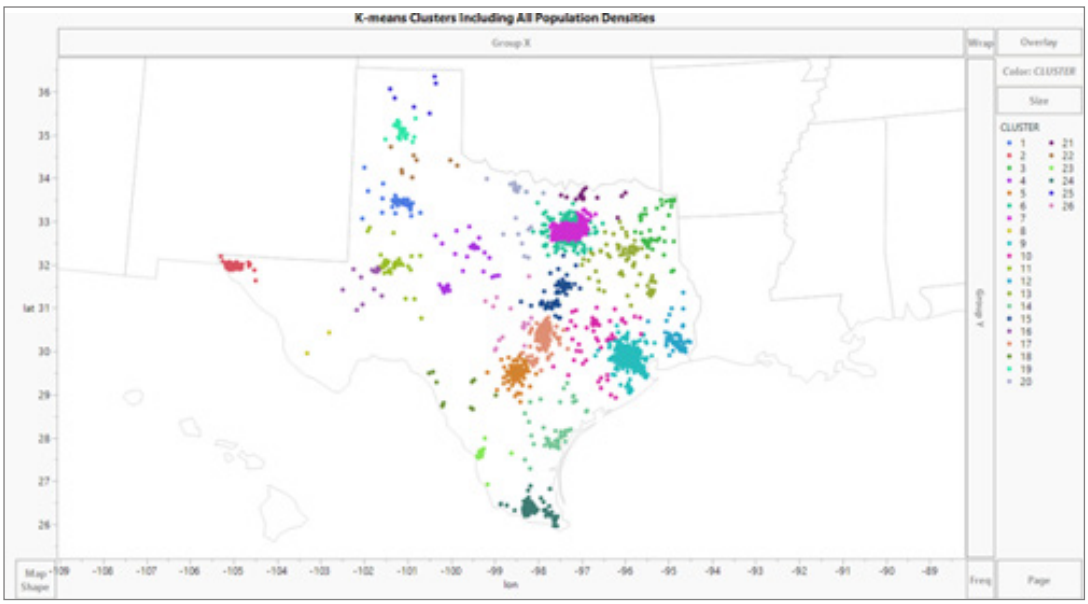


Figure 2. Cluster agents together based on attributes that make good comparison groups.

Anomaly detection finds outliers – agents who seem to be performing statistically differently from their peers – with the ability to drill down to the level of the individual application. Similarly, we may look at time series shift, which may show an unexpected change in activity, such as sharp decline in activity or a spike in commission that may point to an agent gaming the system.

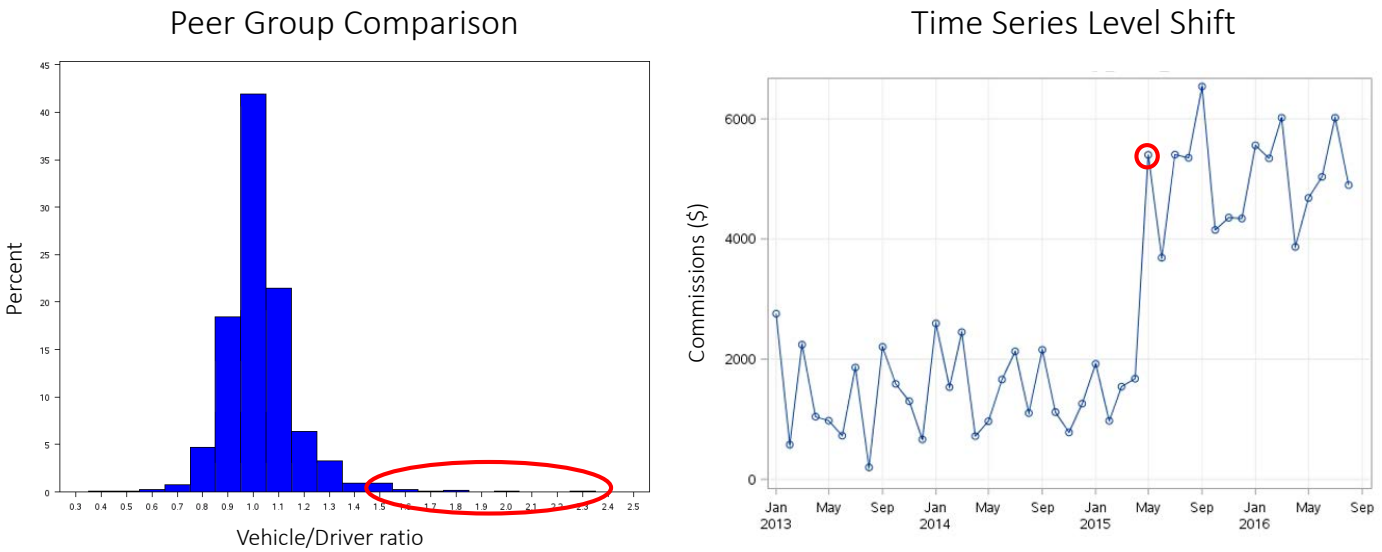
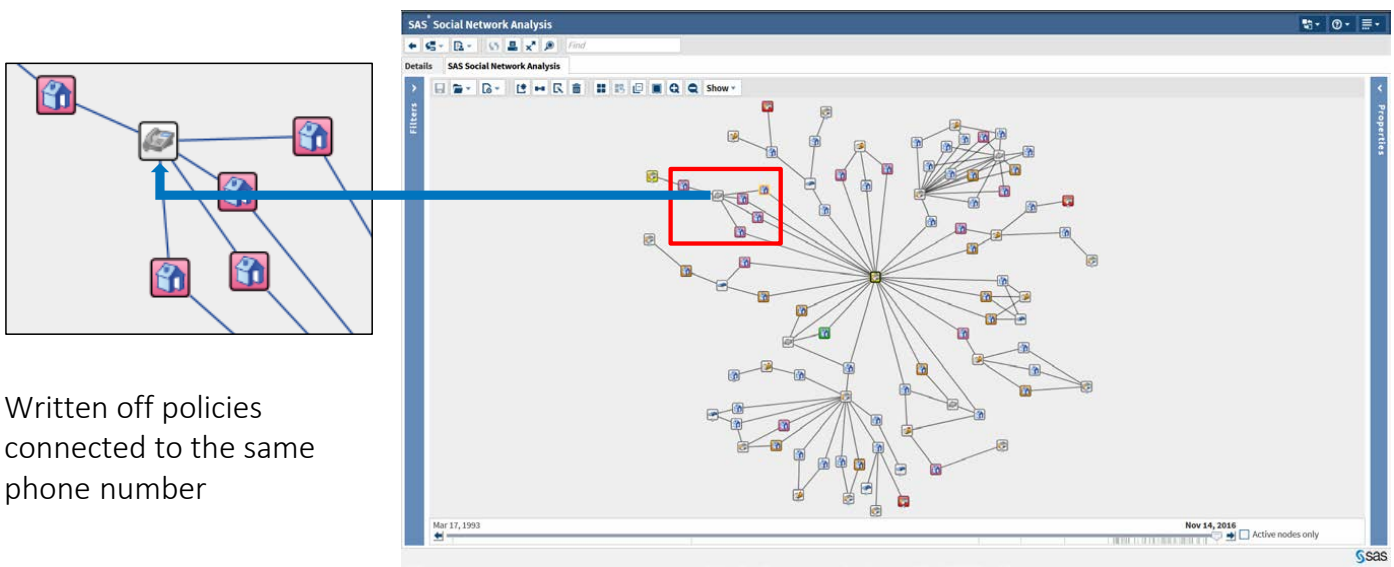


Figure 3. Anomaly detection spots agents whose activity is out of the norm.

Social network analysis, which we also saw in Figure 1, makes links among key entities in the application, such as households, VINs and insured properties. When this social network is oriented around an agent, we can see trends, such as here, where the agent has five written-off policies associated with the same phone number. Did the agent take out policies at the end of one quarter and write them off at the start of the next quarter to make a target?



Written off policies connected to the same phone number

Figure 4. Social network analysis can identify suspicious connections associated with an agent.

Whatever type of analysis is used, the fraud detection system presents the evidence in an easy-to-use interface (for triage or book reviews). The investigator or an auditor makes the decision to accept or decline an application, or look further. In the case of agent gaming, maybe the evidence just suggests the need for additional training rather than passing through to internal audit.

Ultimately the system learns from each experience and its outcomes – the positives and false positives – to continuously improve the analytics each time you run the cycle.

Identify customer gaming at the point of application

Insurers that sell primarily over the telephone or internet are subject to a number of well-known and emerging threats, such as:

- Fronting, such as where a driver with a good record is named as the main driver on an auto policy, when the main driver is actually someone much more high-risk.
- Flipping or "garaging," where different zip codes or postal codes are used to reduce the premium.
- Ghost brokering, where independent agents use alternate identities to get people onto the insurance ladder.
- Getting refunds on canceled policies that were bought with stolen cards.

In many cases, customers don't view this activity as fraud, just playing the system – much like cheating on taxes.

Here's a real-life example. A 24-year-old went on the website of a large, well-known UK insurer to get an auto quote. The first data entry showed him as the only person covered on the policy, with one previous claim, living in London and parking the car on the street overnight. The annual premium is £3,425.

The individual then goes back onto the website and starts to manipulate the information. The IP address of the user's device tells the tale.

Remove the reference to a prior claim, and the premium drops to £2,960. Name a 51-year-old parent with no claims as the primary driver, and the premium drops to £1,026. Get a five-year, no-claims discount for further reduction. Finally, change the postal code away to rural England, and the resulting premium quote is just 13 percent of the original, at £385.

This is an extreme example, but it's happening. Digital application channels make it easy for people applying for automobile and property insurance to learn how to work quotes to their advantage. Unless these manipulations are uncovered, the insured pays less than the real risk he or she represents. The insurance company assumes unanticipated risk, which can have a significant impact on the future pricing of risk and on reinsurance. All for business the insurance provider might not have wanted in the first place.

Analytics can spot this form of gaming in real time, for instance by setting thresholds that define how much an applicant can manipulate the premium before triggering action, such as messaging, callbacks or blocks.

For applications received through a digital device, it is critical to have a high level of assurance that the individuals behind the devices are who they purport to be.

Elements of a solid insurance application and claims fraud solution

And **end-to-end** solution that spans the entire process from application submission through claims to final disposition and reporting.

Data integration from internal and external sources, such as device profiles, public records and portfolio data for existing, closed and previously declined accounts, customers and applications.

Advanced analytics to extract insights from the available data, including rules, anomaly detection, models and network link analysis.

Approve/refer/decline decisions offered in **real time**, **near-real time** or batch modes, depending on rules violated or model score.

A flexible and configurable user interface that presents all the information needed for decisions or investigations in **one intuitive portal** – with the ability to track and append the record as the process uncovers new information.

User-defined reports and **data visualizations** in numerous formats, including graphs, charts and network diagrams that uncover patterns.

Application fraud analytics in action

Insurance companies that have invested in strong anti-fraud capabilities have seen results. For example, SAS partnered with a large US carrier to deploy a solution to identify agent gaming and increase the productivity and throughput of field underwriting, territory managers and internal audit teams.

Using analytics to improve detection, the solution found 10 times more bad-performing agents – 40 percent referred to internal audit, compared to only 4 percent under the legacy process. At the same time, analysis and investigation efficiency improved by 13 hours, and data gathering efficiency improved by two hours.

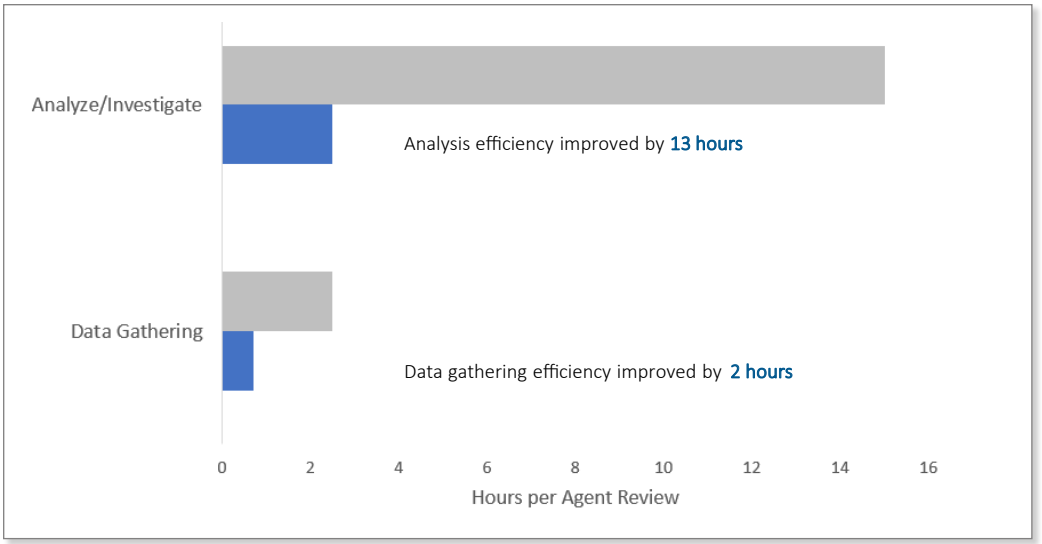


Figure 5. Analytics found more agent gaming while improving investigator efficiency.

The company can now do five investigations in the time it formerly required to do one, because the data has been brought together, the analytics deliver more meaningful alerts, and the audit team can focus on their core work rather than on data housekeeping.

Ultimately, a robust application and claims fraud solution shuts the front door before fraud has a chance to get in and get started.

Learn more

sas.com/en_us/software/detection-investigation-for-insurance.html

To contact your local SAS office, please visit: sas.com/offices